

Windows Management Experts is a leading rapid and responsive Microsoft solution integrator that helps direct customers and partners realize the full benefits of their existing Microsoft investments through a number of solutions in the areas of M&A migration services, Power Platform, Endpoint Management, Microsoft Security & Compliance and Azure services. In our practice we found that roughly 30% of our clients use only 40% of the overall features with the licenses they are already paying for. The value we provide is in closing that gap so the full realization of the Microsoft technology stack is captured, adopted and benefited throughout the organization.

Windows Management Experts Microsoft Security Evaluation

WME Helps You Maintain Your Security-Related Certifications

- Though Azure and Microsoft 365 already offer comprehensive compliance offerings that can help organizations meet their regulatory requirements, WME security evaluation offerings provide a much-needed boost to your compliance-related risk handling, improvement to security-readiness, and sensitive data protection.
- Plus, organizations need some strong professional backing to be sure of their vital assets' ultimate safety and earn/maintain their widely acclaimed security standards. At WME, we are proud of our "Secret Sauce" Security Evaluations based on the latest security best practices and some WME-exclusive techniques.
- We also use customized & propriety tools to help organizations with their own security perspective and automate their systems to have their entire infrastructure reach a level of compliance so that they can adhere to any crucial security-related certifications.
- We also use some native tools provided by the hyper scalers and have a unique AD Automation blueprint that we create for your security auditors so that they can run future security evaluations on their own.
- We also assist your organization get/maintain 120+ plus compliance certifications for Microsoft Azure and Microsoft Office 365. Moreover, we provide you with ongoing support to help your team comply with these standards. We deliver all these services by conducting regular audits, building comprehensive dashboards with user-oriented metrics, and training your employees on security best practices.

Some Examples of Compliance Certifications:

SOC 2 Compliance: We provide a detailed assessment of your Azure and Microsoft 365 environments to identify potential SOC 2 (**Systems and Organization Controls 2**) compliance gaps. We then work with your team to implement the necessary controls to close these gaps.

NIST Compliance: We help you implement the NIST (**National Institute of Standards and Technology**) Cybersecurity Framework to improve your organization's overall cybersecurity posture. This would include implementing encryption, access control, and incident response controls.

CSA ISO compliance: We help organizations obtain CSA (**Safety standards in Canada**) STAR certification; an independent assessment of their cloud security controls. This would demonstrate to their customers and partners that they have taken the necessary steps to protect their data.

And 100+ more

Windows Management Experts

Microsoft Security Assessment

What We Provide

1. Identify any malicious users or activities in the environment.
2. Perform a thorough review of all configurations within M365 and Azure.
3. Assess risk factors related to user access controls, application vulnerabilities, and system security settings.
4. Ensure proper data governance policies are in place.
5. Provide recommended best practices and other areas to be reviewed to secure your services.
6. The time frame for completion is one week with reporting to the delivery team approximately five days.

What We Do

1. **Collect data** - Define data collection process.
 - a. Consultant direct access to environment and will install and run scripts to collect data.
 - b. Consultant executing the tasks with customer "over the shoulder" monitor.
 - c. Customer executes the steps with technical consultant oversight.
2. **Collate data** - Technical consultant will parse, consolidate, and organize data for analysis by the tools.
3. **Create report** - a multiple excel spreadsheet will be create provide a comprehensive view of all the components in the environments along with noted risks in a high, medium, and low ranking. Report includes recommendations on what needs to be done to accomplish various certifications (Zero Trust, HIPAA, SOC2, etc.)
4. **Review report and finding** - this includes 1-2 hours review of the findings and a discussion of potential next steps or action the customer may want to take based on the review.
5. **Remediate** any agreed upon and discovered critical or high-risk intrusions or settings/configurations that were discovered and reported in the scan/findings.

What You Get

1. A multi-tab Excel workbook with results of scans and list of security risk and comprehensive recommendations
2. A one-to-two-hour review of the Findings Report

Case Study # 1 >> Security Evaluation, Remediation, and Implementation

Client Industry: Banking

Client Environment: Microsoft 365 and Azure

The Problem/Opportunity:

- Customer requested a security scan and evaluation of their entire infrastructure.
- They required us to implement the results of the scan/evaluation.
- Customer also asked us to assess the potential damage of a security breach of a user's account right before they requested the evaluation.

The WME Solution:

- Due to the recent security breach, we first used tools including eDiscovery to assess what happened and the potential damage including the data loss that had been done.
- We identified what areas and data elements did the bad actors gain access to and provided recommendations on how to remove the security vulnerabilities.
- During this entire engagement, we identified all the IP addresses that were used by the bad actors to gain access to the client's M365 environment and blacklisted them all.
- As a custom action, we turned Geo fencing on for all users. We also reported all the data areas that could have been accessed by the bad actors. We also gave an abstract report on the categories of data they were interested in.
- Due to the criticality of the matter, we completed the whole task in just two weeks rather than a typical four to six weeks.

Windows Management Experts

Microsoft Security Assessment

- Based on the results of that scan, we implemented all high-priority and critical recommendations as well as all low-impact recommendations.
- As a standard practice, we also shared metrics-based reports to describe the progress we were making daily.
- To ensure an uninterrupted environment, while we implemented efforts to solve client's problem, we used an Agile type of daily call to review the last 24 hours' progress and present to client what would be done in the next 24 hours.

Challenges We Faced & Solved

Challenge # 1: The hardest challenge was to complete a highly sophisticated security scan and remediation task in just two weeks. Whereas such tasks typically take at least 4-6 weeks of tedious work.

Challenge # 2: Another challenge was to satisfy the customer's demand to monitor and get involved with the effort which we normally do by ourselves.

The Final Outcome: Finally, the customer was 100% satisfied with the results WME provided. We were able to move the customer's Overall Compliance Score from 21% to 99%.

Case Study # 2 >> Security Evaluation, Maturity, and Implementation

Client Industry: Engineering

Client Environment: Microsoft 365 and Azure

The Problem/Opportunity:

- The customer requested a security scan and evaluation of their entire infrastructure.
- They wanted us to implement the scan/evaluation results to secure their system.
- They required us to provide Intune-related services enrolling their devices.
- They also asked us to assess the potential damage of a security breach of a user's account right before they requested the evaluation.
- As they were receiving tremendous spam, ransomware, and phishing attacks, WME had to remediate the whole security vulnerability and restore the environment to an absolutely safe state.

The WME Solution:

- We identified all the exploitations, quickly remediated all the vulnerabilities, and secured the whole environment to increase the Maturity level by two.
- We also provided some high-level support for the organization's staff while transforming their products.
- Using Business Cloud Integration, we designed and deployed Microsoft Security tools and Property tools to allow for quick automation of the platform and migration of the data wherever required.
- We also provided recommendations to cut costs for the client's security measures.

The Steps & Approach We Adopted:

We Provided a Cyber Security

Evaluation: This particular approach was necessary to identify security risks in the client's whole environment. This information was automatically provided as a Segway to prioritize security investments and improve the organization's security posture.

We assisted with providing an updated

organization's maturity level: This metric was used to identify areas where security improvements and continuous monitoring were needed. This information was used to develop and implement a security improvement plan and strategy to automate WME tools.

Preventing Future Cyberattacks:

The implementation of security was defined to help to protect the client organization from cyberattacks. This includes implementing security policies and procedures, implementing security controls, and training employees on security procedures.

The Final Outcome: The client was 100% satisfied with the results we provided. We improved the customer's Overall Compliance Score from 21% to 99%, and their Identity score to 100%.

What it Costs

1. Single Security Scan and Findings Report costs \$5000.