MICROSOFT CLOUD ASSESSMENT

Risk Report

CONFIDENTIALITY NOTE: The information contained in this report is for the exclusive use of the client specified above and may contain confidential, privileged, and non-disclosable information. If you are not the client or addressee, you are strictly prohibited from reading, photocopying, distributing, or otherwise using this report or its contents in any way.

Scan Date: 2025/01/03

Prepared for: Your Customer / Prospect

Prepared by: Your Company Name

2025/03/03

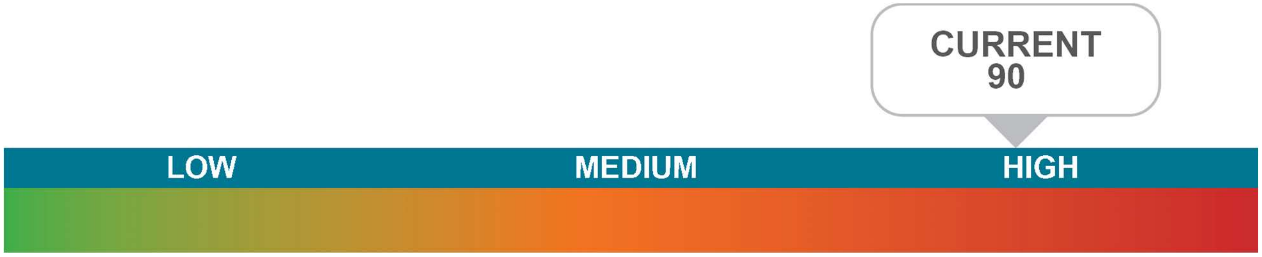
Table of Contents

1 - Overview

The Microsoft Cloud is composed of various components and applications including Azure Active Directory, Microsoft Teams, OneDrive, Outlook and SharePoint. Risks associated with using the Microsoft Cloud are grouped into operational and misconfiguration. Some issues represent improvement in configuration desired to improve the Microsoft Secure Score. Not all changes are necessary for every type of business. A qualified IT professional should always evaluate the benefits of implementing any particular control or recommendation, balancing it with business needs and cost.

2 - Risk Score

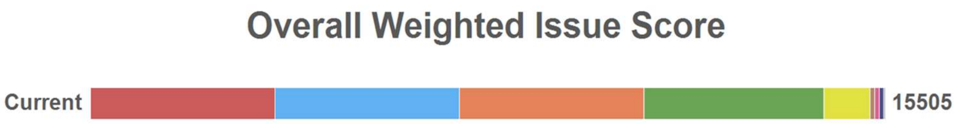
The Risk Score is a value from 0 to 100, where 100 represents significant risk and potential issues. The score reflects the risk associated with the highest risk issue.



Several critical issues were identified. Identified issues should be investigated and addressed according to the Management Plan.

3 - Issues Summary

This section contains a summary of issues detected during the assessment process and is based on industry-wide best practices. The Overall Issue Score grades the level of issues in the environment. An Overall Issue score of zero (0) means no issues were detected in the environment. It may not always be possible to achieve a zero score in all environments due to specific circumstances.



Weighted Score: Risk Score x Number of Incidents = Total points: Total percent (%)

3600 Self Service Password Reset Not Enabled (90 pts each)

Current Score: 90 pts x 40 = 3600: 23.22%

Issue: Unimplemented Microsoft Control: Self Service Password Reset. You have 40 of 40 users who don't have self-service password reset enabled.

Recommendation: With self-service password reset in Azure Active Directory, users no longer need to engage help desk to reset passwords. This feature works well with Azure AD dynamically banned passwords, which prevents easily guessable passwords from being used.

3600 Sign in Risk Policy Not Enabled (90 pts each)

Current Score: 90 pts x 40 = 3600: 23.22%

Issue: Unimplemented Microsoft Control: Sign in Risk Policy. You have 40 of 40 users that don't have the sign-in risky policy turned on.

Recommendation: Turning on the sign-in risk policy ensures that suspicious sign-ins are challenged for multi-factor authentication (MFA).

3600 User Risk Policy Not Enabled (90 pts each)

Current Score: 90 pts x 40 = 3600: 23.22%

Issue: Unimplemented Microsoft Control: User Risk Policy. You have 40 users out of 40 that do not have user risk policy enabled.

Recommendation: With the user risk policy turned on, Azure Active Directory detects the probability that a user account has been compromised. As an administrator, you can configure a user risk conditional access policy to automatically respond to a specific user risk level. For example, you can block access to your resources or require a password change to get a user account back into a clean state.

3510 Legacy Authentication Not Blocked (90 pts each)

Current Score: 90 pts x 39 = 3510: 22.64%

Issue: Unimplemented Microsoft Control: Block Legacy Authentication. You have 39 of 40 users that don't have legacy authentication blocked.

Recommendation: Today, most compromising sign-in attempts come from legacy authentication. Older office clients such as Office 2010 don't support modern authentication and use legacy protocols such as IMAP, SMTP, and POP3. Legacy authentication does not support multi-factor authentication (MFA). Even if an MFA policy is configured in your environment, bad actors can bypass these enforcements through legacy protocols.

900 Multi-factor Authentication Not Registered (90 pts each)

Current Score: 90 pts x 10 = 900: 5.8%

Issue: Unimplemented Microsoft Control: Multi-factor Authentication. You have 10 out of 40 users that are not registered and protected with MFA. See Users section in Azure AD Report for details.

Recommendation: Multi-factor authentication (MFA) helps protect devices and data that are accessible to these users. Adding more authentication methods, such as the Microsoft Authenticator app or a phone number, increases the level of protection if one factor is compromised.

90 On Premise Sync has not occurred in 15 days (90 pts each)

Current Score: 90 pts x 1 = 90: 0.58%

Issue: On Premise Sync has been configured for the organization and is enabled; however, the time since the last sync is greater than 15 days. This may indicate an issue with the on-premise sync.

Recommendation: Investigate and remediate issues with On Premise Sync.

90 Customer Lockbox Not Enabled (90 pts each)

Current Score: 90 pts x 1 = 90: 0.58%

Issue: Unimplemented Microsoft Control: Customer Lockbox Not Enabled.

Recommendation: Turning on the customer lockbox feature requires that approval is obtained for datacenter operations that grants a Microsoft employee direct access to your content. Access may be needed by Microsoft support engineers if an issue arises. There's an expiration time on the request and content access is removed after the support engineer has fixed the issue.

90 Integrated Apps Not Regulated (90 pts each)

Current Score: 90 pts x 1 = 90: 0.58%

Issue: Unimplemented Microsoft Control: Integrated Apps.

Recommendation: Tighten the security of your services by regulating the access of third-party integrated apps. Only allow access to necessary apps that support robust security controls. Third-party applications are not created by Microsoft, so there is a possibility they could be used for malicious purposes like exfiltrating data from your tenancy. Attackers can maintain persistent access to your services through these integrated apps, without relying on compromised accounts.

25 Teams guests allowed to create and remove channels (25 pts each)

Current Score: 25 pts x 1 = 25: 0.16%

Issue: Team settings allows guests to create and remove channels. This could cause loss of data as guests add and remove channels.

Recommendation: Verify if guest creation and removal of channels is desired on the specified Teams. When not necessary, disable the ability of Team guests to create and remove channels to avoid potential data loss and channel proliferation.