M 365 Tenant Review Description

Purpose

The cb20 engineer will walk us through an informal review of the **Microsoft 365** tenant to provide a high-level evaluation of the environment with a focus on security and compliance, optimizing costs, and ensuring the customer is leveraging the full potential of the platform. It will help to maximize the value of the Microsoft 365 investment and support the organization's productivity, growth, and initiatives.

Microsoft has been rapidly evolving the platform, so a periodic review is recommended even if the initial deployment was done per the current best practices at that time. Strategies for security continue to evolve, and its possible new capabilities have been added to the tenant but not turned on. We often see new configurations attempted or partially deployed but not fully backed out properly, leading to security gaps. At the very least, this process is a verification that the current deployment is sound.

Deliverable

The process will include:

- Conducting a screen sharing session with the customer administrator where the cb20 engineer or the customer administrator can control the screen.
- A review of licensing will be done to understand what capabilities the customer is licensed for.
    - If we can receive the licensing ahead of time, we will be more productive.
- As topics are covered there will be brief discussions and configuration spot checks to understand the status of each topic.
- The customer is encouraged to ask questions throughout the process, cb20 is here to share information as much as we are to gather it.
- The duration of the walkthrough is typically one hour and is a no fee activity.
- **Tenant Review Engineering Report**: Findings will be documented and presented once the cb20 team has reviewed.

Topics Covered

- Licensing optimization
- Tenant base security: DKIM (DomainKeys Identified Mail), SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication, Reporting, and Conformance)
- Audit logging: Track and monitor user activities, security events, and data access
- Account Management and Password Policies
- Azure AD Identity Management: Identity Protection, MFA, Conditional access
- DLP (Data loss Prevention), AIP (Azure Information Protection)
- Defender security capabilities: server, email, endpoint
- Use of secure score
- Secure external sharing
- Device and Mobile Device Management
- General upkeep and forward-looking topics (i.e., the removal of Legacy Protocols)

NOTE: This M 365 only, Azure Tenants require a different set of services depending on the workloads.