ManageEngine
O365 Manager Plus

OIG's Office 365 audit checklist and how to prepare for it.

www.o365managerplus.com

Introduction

Since its inception, the US Department of Health and Human Services' Office of Inspector General's (OIG) mission has been to fight waste, fraud, and abuse. With the rise of software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS), the OIG has ramped up enforcement to ensure federal agencies and federal contractors that transmit federal Controlled Unclassified Information (CUI) are following policies set by the National Institute of Standards and Technology (NIST). OIG audits are one way the OIG can ensure organizations are complying with those policies.

Over 80 percent of the federal agencies use Microsoft Office 365, Azure AD, and collaboration products such as SharePoint, Yammer, and Teams to serve their thousands of employees and contractors. It is of paramount importance for them to protect sensitive information that's residing in these platforms to comply with the NIST recommendations.

In this e-book, we will discuss how to set up Office 365 to ensure your tenant holds up in an OIG (Office of Inspector General) audit.

What will be examined during an OIG audit

The three security aspects that will be examined during an OIG audit include:

- Security of personally identifiable information (PII)
- Implementation of multi-factor authentication (MFA)
- Retention policies

Personally identifiable information (PII)

According to the NIST, PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

PII security in the US Securities and Exchange Commission (SEC): The OIG's observation

The US Securities and Exchange Commission (SEC) was recently audited by the OIG, and the SEC was found to have not stored PII information correctly. From the audit report:

"In addition, in at least five instances, agency personnel had not enforced contract requirements related to safeguarding personally identifiable information (PII) even though experts had access to PII, including investors' names, addresses, dates of birth, and customer account information. We also found that contracts lacked controls regarding the inadvertent release or disclosure of information after the SEC transmits information to experts. As a result, the agency lacked assurance that experts and their information systems achieved basic levels of security to protect the SEC's sensitive, non-public information, including PII. We did not identify instances in which unauthorized individuals accessed such information after it was provided to experts. However, the agency should take steps to minimize the risk of unauthorized disclosure, modification, and use of its sensitive, non-public information provided to experts."

How to secure PII in Office 365

Compliance management features in Office 365 will help you monitor and control who has access to PII to secure access to your PII. However, it lacks real-time alerts. What's the solution? An Office 365 administration, management, and auditing tool like O365 Manager Plus.

Email continues to be the most popular medium for business communication, and a simple means through which employees can share data. ManageEngine O365 Manager Plus identifies emails with PII and other insider information. Once you save the criteria of the emails to be identified, the tool sends you the search results at regular intervals straight to your inbox.

Learn how to run a content search in Office 365 using O365 Manager Plus.

Multi-factor authentication (MFA)

According to the NIST, MFA is using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

MFA settings in the Unites States Department of Energy (DOE): OIG's observation

The OIG is very strict towards organizations that don't protect their data access with multi-factor authentication. In a recent audit of the Unites States Department of Energy's (DOE) system, the OIG stated:

"The weaknesses identified occurred, in part, because officials had not fully planned for implementation of multi-factor authentication on information systems. Department guidance and requirements related to multi-factor authentication technologies also were not always communicated effectively. Without development and implementation of a Department-wide multi-factor authentication process, the Department's information, including sensitive data, will continue to be at a higher-than-necessary risk of compromise. We have made recommendations that, if fully implemented, should help the Department enhance its cybersecurity posture through effective implementation of multi-factor authentication. Management concurred with the report's recommendations and indicated that corrective actions had been initiated or were planned to address the issues identified in the report."

How to manage Office 365's MFA settings

The Micrososft Office 365 Admin Center gives administrators the option to enable or disable MFA for multiple users at a time. However, the choice of selecting the verification methods rests in the hands of the end users.

On the other hand, O365 Manager Plus lets administrators enable, disable, and configure the authentication methods for multiple users—no special privileges or additional premium license needed. Administrators can even delegate MFA management to help desk technicians using custom delegation features without compromising security. O365 Manager Plus even provides an exclusive set of built-in audit reports to closely monitor technicians' activities.

Learn to configure MFA for Office 365 using O365 Manager Plus.

Retention policies

Retention policies help with deleting unnecessary items and/or retaining important data for forensic analysis. They can be applied to a whole organization, a group of users, a single mailbox, or a site.

Retention policies are also used to scan emails and other item types in the Recoverable Items folder. By default, if no retention policy is set, the data will be deleted in 14 days. This time period can be increased to a maximum of 30 days, beyond which the items are purged. After this period, items are deleted and cannot be recovered. Users can purge items on their own, but with a retention policy protecting such files, the administrators will still be able to access this data using eDiscovery or Search-Mailbox.

As these retention policies can either preserve or delete content, it's important to know what happens if more than one policy is applied on a single item. There is a set priority among retention rules: the most important rule is that retention always takes precedence over deletion, and if more than one retention applies to an item, the one with the longest retention period wins.

Example: There is an organization-wide retention policy that protects data younger than five years old and another organization-wide policy that deletes all items older than two years. Items created three years ago will not be deleted because of the first policy, while items older than five years will be deleted because of the second policy.

Only users with appropriate permissions can create and manage retention policies. There are two default role groups that have permissions to manage retention policies: Compliance Administrator and Organization Management.

Learn to place Office 365 mailboxes on retention hold and apply retention policies using O365 Manager Plus.

How to configure retention policies in Office 365

Depending on the regulations an organization is required to follow, it'll have different retention schedules for emails, financial statements, voicemails, and documents. This can be a burden if documents and emails have not been tagged correctly.

Office 365's retention tags are used to specify how long a message remains in a mailbox and the action to be taken when the message reaches the specified retention age. When a message reaches its retention age, it's moved to the user's In-Place Archive or deleted. To apply one or more retention tags to a mailbox, you must add them to a retention policy and then apply the policy to mailboxes.

With O365 Manager Plus, administrators can place the mailboxes of users who have gone for a vacation on retention hold, and retain the deleted mailbox items for the specified number of days irrespective of the retention policies applied to the mailbox items.

Learn how to place mailboxes on retention hold using O365 Manger Plus.

Takeaway

Preparing for an OIG audit, or any compliance audit for that matter, is a continuous, time-consuming, and resource-intensive process. In most cases, the OIG will schedule an onsite follow-up to ensure that all violations have been addressed, so make sure you understand the requirements clearly.