EGNYTE

The Admin's Guide To M365 Security And Compliance

A Handbook For IT Teams

Contents

Introduction

With so many high-profile data breaches, and a growing number of regional regulations designed to protect both corporate and personal data, the topics of security, compliance, and governance have become a priority for many executives. The General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) are two examples of these new regulations that include strict governance policies, broad mandates, and strict fines. As a result of this widespread change, organizations are spending more time evaluating the features and controls of their IT solutions in an attempt to decrease risk.

As with any other enterprise solutions, Microsoft 365 and each of its individual workloads will likely undergo some degree of scrutiny. The platform supports global customers, each with regional and differing standards and regulations surrounding intellectual property (IP) protections. With so many new and changing standards around the world, Microsoft is constantly updating the list of compliance and security standards that they support.

Microsoft works hard to comply with these standards and regulations in the creation, delivery and support of its own solutions — this does not mean that by using Microsoft 365 your own organization is automatically secure, compliant, or well-governed. It is important for organizations to understand their own local, regional, or global requirements and how these requirements are met (or unmet) by the platform's out-of-the-box capabilities.

The purpose of this ebook is to provide an overview of the primary security, compliance, and governance capabilities of the Microsoft 365 cloud platform, and help your organization better manage your business requirements and mitigate any risks.

Microsoft works hard to comply with these standards and regulations in the creation, delivery and support of its own solutions — this does not mean that by using Microsoft 365 your own organization is automatically secure, compliant, or well-governed.

Common Compliance, Security, and Privacy Concerns

The Microsoft 365 cloud platform is managed and controlled by Microsoft. Out of the box, core capabilities protect and handle perimeter and edge access and data. These tools are built into the platform and provide you the organization default protections that do not require any support or configuration.

Within the service are extra capabilities that protect either at the application, service, or content level, requiring deployment planning and configuration. Even with these capabilities, many organizations struggle to implement, utilize, or monitor using the tools.

Microsoft is constantly reviewing and revising the platform's security, compliance and governance capabilities, and the various standards and regulations that it complies with. As with any enterprise application, there may be feature gaps within the requirements for your industry, for specific Line of Business (LOB) application integrations, or some other legacy business rules or system automation.

Top M365 Security Considerations

Security is always a concern for every organization. Knowing the current security posture, which controls to implement, or even if the current protections are adequate, are critical to security. Microsoft 365 provides out-of-the-box managed security controls and multiple features based on licensing. Worrying about the security of an application or service is not unique to using Microsoft 365.

Below are critical areas of focus that organizations must consider:

1 Unauthorized Access	Access control and management is always an area of worry for all organizations. Providing an easy to use yet secure access control platform is more complicated than merely providing usernames and passwords. Organizations need to provide such things as a second factor, biometric login, including authorizing users after completing login. The core problem is organizations knowing that the currently logged in user is the expected user and not a malicious actor.
2 Compromised Machine / Asset	With many of the current attacks, they are often successful due to compromising devices within the organizational network. Attackers can then perform other attacks and actions, hiding them within regular network traffic. Organizations need to provide a platform that can either restrict these actions on devices or block unauthorized Access completely.
3 Data Theft / Espionage	Though well-known, theft or Espionage are long-standing risks that are not always thought of when reviewing security. For various reasons, Espionage is explicitly still regarded as affecting governments or large organizations which potentially have information that could affect more than just the business. However, this is on the increase, along with Data Theft, involving all organization types and sizes. All organizations need to implement protections for controlling the dissemination of digital data and physical assets.
4 Denial of Service	With organizations moving to the cloud for better scalability and services, denial of service attacks become a reality. In the past, with organizational data stored locally, rarely were denial of service attacks issued against private networks due to not having access. However, with everything stored in the cloud, a large-scale denial of service attack against the cloud provider could also affect an organization's access and data.

5 Malware or Malicious Code	Malware and Malicious Code are some of the most common entry points for attackers to use. The attacker's objective is to get the unsuspected user to download or execute malicious code or malware. By performing this action, attackers can gain access to not only data but system access. Organizations need to provide protections to block both malware and malicious code from executing.
6 Reconnaissance, Scans or Probes	Part of attacking an organization typically involves reconnaissance, which primarily consists of scanning and probing a network. The goal of this is to identify potential entry points. Organizations can utilize Firewall and Blocking technology to help protect from these types of actions.
7 Policy Violations or Improper Usage	Most data breaches involve internal users who violate an existing policy or utilize software, hardware, or services that are not allowed within all organizations. Most end-user caused breaches are not malicious but the outcome of improper use or lack of protections. Organizations need to implement all security controls that can monitor and protect applications and services.

Top M365 Compliance Considerations

Organizations around the world struggle with the incredible growth of data within the enterprise – and the fact that their data is spread across so many different systems and applications. Compliance is a concern for nearly all organizations, whether it be complying with regulations or specific company policies and controls.

Below are the top compliance considerations for data in M365:

1 **Monitoring**	The ability of an organization to know if the content meets regulatory compliance policies is critical. If an organization can identify potential policy violations or issues using monitoring, it can control potential data leaks.
2 **Archiving**	Removal or saving of content and data long-term can have an impact on compliance and security. The more data or content that is available increases the security footprint for organizations. Providing a process for securely archiving content as well as deletion can mitigate this issue.
3 **eDiscovery**	In the event of a legal challenge, organizations must provide the ability to place content on hold and perform discovery investigations. This ability allows organizations to identify and organize content into what is required and what should be submitted. When combined with archiving and deletion policies, only relevant content will be visible during eDiscovery.
4 **Automation**	The key to an excellent compliance implementation is to automate as much of the process as possible. Allowing end-users to make decisions on critical data can lead to problems. Using automation solutions or services can minimize issues by automatically removing the need for end-user interaction.
5 **Protection, Retention, and Recovery**	The ability to protect content with security policies, retain and recover if needed, ensure better management and control of all organizational data. Providing a mechanism to classify content, which applies security controls manually or even better automatically, allows organizations to control data dissemination.
6 **Standards and Certifications**	All organizations are required to meet specific corporate or legal standards for all content and applications. Each organization, though unique in the particular standards or policies, needs the ability to validate compliance.

Top M365 Privacy Considerations

Privacy is the outcome of both Compliance and Security controls. An organization must understand its privacy needs and implement specific tools, services, and management. By combining Microsoft 365 Security and Compliance controls, organizations can meet their privacy needs.

Below are the top privacy considerations for data in M365:

1 **Implementing Data Privacy**	Deployment of Data Privacy requires a combination of controls for both compliance and security. Organizations need to plan out the process for achieving either company or regulatory privacy by combining both deployments, which will achieve data privacy.
2 **Proliferation of Devices**	With the advent of Bring-Your-Own-Device (BYOD), organizations worry that company data could be easily copied to devices not managed or owned by them. All organizations need to implement either fully managed devices or application protections to control data dissemination onto non-organizational devices.
3 **Increased Maintenance**	There is a perceived issue with implementing any privacy controls, which is the amount of effort required. It is correct that real data privacy does require increased management and maintenance, which is a common concern raised by all organization types and sizes.
4 **Complicated Access Control**	Implementing access control is not as simple as providing a login platform. Single-sign-on into multiple applications and services requires extensive planning and configuration. When moving to the cloud, organizations need to accommodate this type of platform to ensure that they can access the necessary applications.
5 **Visibility into Data**	Knowing what happens to organizational data, where it goes and is classified is an essential part of security and data privacy controls. Microsoft 365 provides visibility into data; however, it does require configuration and implementation. All organizations need visibility into disseminating data to ensure that either company or personal data is not leaving the network's protection.

6 **Ever-increasing Scale of Data**	Over the past few years, organizations have seen exponential growth in data stored within applications and services. With so much data being stored, managing and monitoring is much more complicated and requires specific tooling. It can often be a deployment blocker when organizations have too much data.
7 **Regulatory Compliance**	Meeting specific regulations is a complex task for any organization. Firstly, understanding the regulation and mapping it to the precise control and features within Microsoft 365 is time-consuming and often complicated. Though Microsoft does provide tooling to assist with the implementation, many organizations struggle with this and do not meet the regulations.

Microsoft 365 Security Architecture

Microsoft 365 provides various security capabilities at the core tenant level and within each service and application. Most security controls depend on each other and are hierarchical. Each control fits into either Security and Privacy or Data Protection tools. Outside of these two core categories of controls, edge controls provide protection automatically within the Microsoft 365 Data Centers.

The most critical part of implementing security controls within Microsoft 365 is licensing. Based on the selected or available licensing, some controls are not available, or features are limited.

Security and Privacy Tools

Security and Privacy are a core part of any organization's security posture. The ability to limit who can log in, when they can log in, and control how they log in or gain access are vital steps to the tenant's overall security. Understanding the available features and services, then when and if to enable, will help create a more secure tenant.

Authentication and Access Controls

The first step into securing Microsoft 365 is to control authentication into the tenant. All authentication flows through either the Microsoft Login Portal, On-premises Login, or Cloud Federated Platform. It provides a common way for accounts to authenticate and get checked against access controls. A simple example of this is to block access to all logins that don't come from specified IP Addresses. There are, however, multiple controls that can inspect and control the login process.

Security and Privacy are a core part of any organization's security posture.

The critical controls for this are:

1. Multi-Factor Authentication
2. Banned Password Lists
3. Removal of Password Expiration
4. Azure Privileged Access / Account Management
5. Azure Identity Protection
6. Network Blocking using IP Addresses and Ranges
7. Inactive Session Sign-out
8. Self Service Password Reset
9. Account Lockout Threshold

Each control will either allow or block access, limit access, control passwords, account lockout, and force different account management processes. The most critical controls to implement are:

Multi-Factor Authentication

In nearly every Data and Security breach involving a compromised account, simply enabling Multi-Factor Authentication would have blocked the attack. Forcing every authentication request to validate a second factor, such as using an SMS or Token, will limit any malicious actors' ability to use the account. Best practice dictates not to use SMS/Text messages where possible, as this has been under attack for a long time and is not as secure as it once was. Require end-users to install an Authentication app on their mobile devices that push the device's request where they can approve as needed. These applications also provide in-time tokens that last a specific time and are available in situations where push notifications are not appropriate or cannot work.

Banned Password Lists

Default global banned password lists automatically apply to all users in an Azure Active Directory Tenant. Azure Active Directory continuously analyzes telemetry data looking for commonly used weak or compromised passwords. Simple or Weak passwords get added to the global banned password list. Organizations can also define entries in a custom banned password list. When users change or reset their passwords, the current version of the global banned password list validates the password's strength. The global banned password list applies automatically to all users in an Azure AD tenant. There's nothing to enable or configure, and it can't be disabled.

Removal of Password Expiration

When enforcing periodic password resets, passwords become less secure. Users tend to pick a weaker password and vary it slightly for each reset. This type of behavior can often lead to the re-use of existing passwords, as well as malicious attackers guessing the password. Suppose a user creates a secure password (long, complicated, and without any pragmatic words present). In that case, it should remain as strong in 60 days as today—the recommendation by the National Institute of Standards and Technology (NIST) to disable password expiration. The guidance is only to force a change or update a password if an account is confirmed as compromised. Azure Active Directory provides the ability to set password expiration policies and disable them for specific users or all users.

Account Lockout Threshold

Many successful account compromises happen because simple protections aren't defined. The most common is the number of times passwords are entered incorrectly before locking the account. The higher the number, the more times a malicious actor has to guess the password freely. Azure Active Directory Smart lockout uses cloud intelligence to lock out malicious actors trying to guess end-users' passwords. The intelligence platform recognizes sign-ins from valid users and treats those differently from those that attackers and other unknown sources. The smart lockout can lock out the attackers yet still allow users to continue to access their accounts. Smart lockout is on by default within all Azure Active Directory instances; however, organizations can customize them as needed. The default setting is ten failed sign-ins, with the recommendation to set lower as required and in conjunction with the organization.

Conditional Access Policies

Conditional Access is the Azure Active Directory tool to bring signals together, make decisions, and enforce organizational policies. Conditional Access is at the heart of the identity-driven controls. Conditional Access policies are simple if-then statements; if a user wants to access a resource, they must complete an action. Conditional Access analyzes signals such as user, device, and location to automate decisions and enforce organizational access policies for a resource. Conditional Access policies can apply controls like Multi-Factor Authentication (MFA). The most common Conditional Access policy that is required is to block legacy authentication. Legacy protocols are POP, SMTP, IMAP, and MAPI, and cannot enforce any second-factor authentication, making them preferred entry points for malicious actors attacking the organization.

More than 99 percent of all password spray attacks within Azure Active Directory utilized legacy authentication. To add, more than 97 percent of all Credential Stuffing attacks against Azure Active Directory also used legacy authentication.

Cloud App Security

Microsoft Cloud App Security is a Cloud Access Security Broker (CASB) that supports various deployment modes, including log collection, API connectors, and reverse proxy. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyber threats across all your Microsoft and third-party cloud services.

Visibility
Help detect all cloud services; assign each a risk ranking; identify all users and third-party apps able to log in

Data security
Identify and control sensitive information (DLP); respond to classification labels on content

Threat protection
Perform adaptive access control (AAC); provide user and entity behavior analysis (UEBA); mitigate malware

Compliance
Supply reports and dashboards to demonstrate cloud governance; assist efforts to conform to data residency and regulatory compliance requirements

Organizations need to protect users and confidential data from the different methods employed by malicious actors. Cloud App Security and other CASB Solutions help you do this by providing a wide array of capabilities to protect the environment.

Using the Cloud App Security Framework, organizations can discover and control Shadow IT's use, protect sensitive information anywhere in the cloud, protect against cyberthreats and anomalies, and assess any cloud apps' compliance.

Data Protection Tools

Microsoft 365 provides core capabilities for data protection. Organizations need to comply with business standards and industry regulations by protecting sensitive information and preventing its inadvertent disclosure. Sensitive information includes financial data or personally identifiable information (PII) such as credit card numbers, social security numbers, or health records. Data protection within Microsoft 365 starts by using Sensitive Information Types and Labels, which are also available within Data Loss Prevention policies.

Data Loss Prevention provides edge protection for all content either entering or leaving the organization. It is often referred to as the safety net to catch all data trying to exit the organization, whether intended or malicious. A Data Loss Prevention policy identifies specific content and provides the security controls to encrypt or even block.

The building blocks for identifying any sensitive or personal data is through the use of Sensitive Information Types.

Sensitive Information Types

Data Loss Prevention (DLP) within Microsoft 365 includes many sensitive information types ready to use in DLP policies. A sensitive information type is defined by a pattern that can be identified by a regular expression or a function. Corroborative evidence such as keywords and checksums assist in identifying a sensitive information type. Confidence level and proximity are also part of the evaluation process.

Sensitive Information Types fit into one of three categories: Financial, Medical, and Health and Privacy. Organizations can also create custom types that match specific content that is unique to the organization. Data Loss Prevention (DLP) includes over eighty sensitive information types ready for use in DLP policies.

Sensitivity Labels

Sensitivity labels within the Microsoft Information Protection solution allow the classification and protection of the organization's data. These labels provide the following high-level capabilities:

- Provide protection settings that include encryption and content markings
- Protect content in Office applications across different platforms and devices
- Protect content in third-party apps and services when using Microsoft Cloud App Security
- Protect containers such as Microsoft Teams, Microsoft 365 Groups, and SharePoint sites
- Extend sensitivity labels to third-party apps and services
- Classify content without using any protection settings

Sensitivity Labels allow for content encryption, marking the content using watermarks, general content protections no matter where the content resides, and automatically applying labels to content. Usually, the labels are applied manually by end-users; however, automatic processes can tag the content and use the required protections without any user intervention.

Labels are available to use on their own or combined with other labels and added to a policy. Sensitivity Label Policies contain the restrictions and controls and apply to content matching the labels.

Data Loss Prevention

Data Loss Prevention (DLP) provides edge protection for all content either entering or leaving the organization. It is often referred to as the safety net to catch all data trying to exit the organization, whether intended or malicious. A Data Loss Prevention policy identifies specific content and provides the security controls to encrypt or even block.

A Data Loss Prevention (DLP) policy contains the conditions to be met, along with the required protections and actions to perform. DLP policies are applied to sensitive items across Microsoft 365 locations and scoped further based on properties and values. The rules are what enforce any business requirements for the organization's content. A policy can contain one or more rules, and each rule consists of both conditions and actions.

Conditions are necessary because they determine what types of information you're looking for and when to take action. Conditions also focus on the content, such as the type of sensitive information, the context, and the sharing direction. You use conditions to assign different actions to different risk levels.

When content matches a condition in a rule, you can apply actions to protect the content automatically. When content matches the rules and conditions, end-users and compliance administrators, or any specified user receives an alert.

M365 Security Metrics

Measuring the organization's security posture is critical to protecting end-users, data, and systems. Microsoft 365 provides three core capabilities to examine the tenant and offers actionable tasks to increase the current security posture.

1. Secure Score
2. Compliance Score
3. Compliance Manager

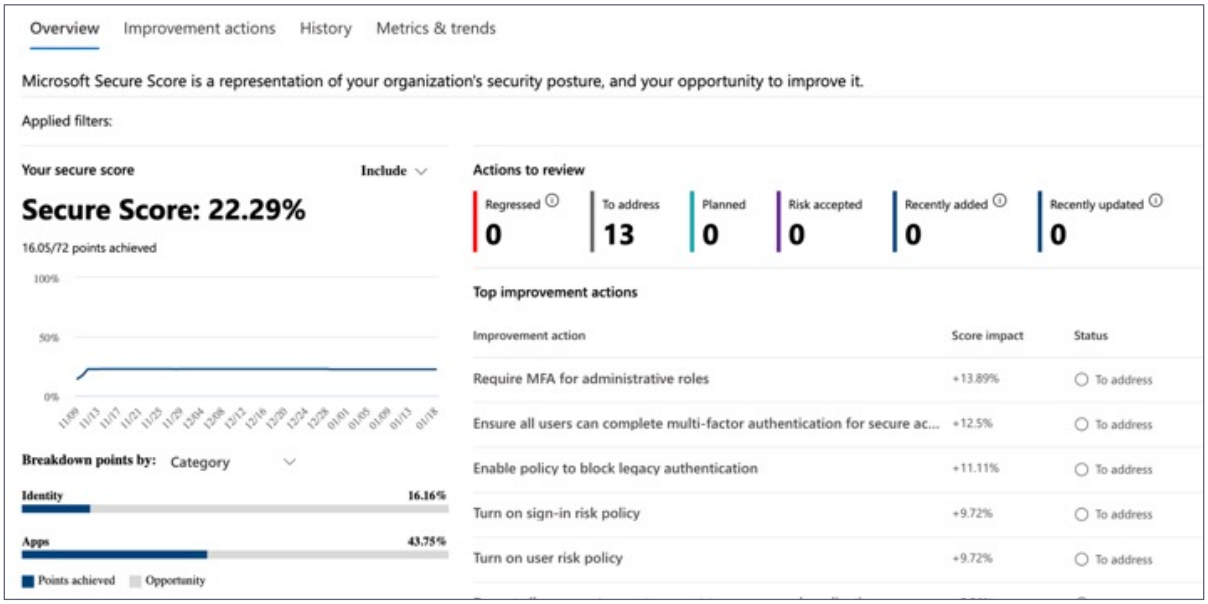
Metrics allow organizations to quickly see the high-priority tasks that will increase the current score and those that may not.

Secure Score

Secure Score helps organizations:

- Report on the current state of the organization's security posture
- Improve their security posture by providing discoverability, visibility, guidance, and control
- Compare with benchmarks and establish key performance indicators (KPIs)

Organizations gain access to visualizations, metrics, and trends and score comparisons with similar organizations. The score also reflects when third-party solutions have resolved recommended actions.



The organizational score displays a percentage of the number of points achieved out of the total possible points. Organizations are also able to view planned score, current license score, and a possible score.

The improvement actions are the security recommendations that address possible attack surfaces. You can also view step-by-step instructions to complete the improvement activities, the improvement activities' current implementation status, and any links to learn about specific actions.

Rank	Improvement action	Score impact	Points achieved	Status	Regressed...	Have license?	Category	Product
1	Require MFA for administrative roles	+13.89%	0/10	To address	No	Yes	Identity	Azure Active Directory
2	Ensure all users can complete multi-factor authentication for ...	+12.5%	0/9	To address	No	Yes	Identity	Azure Active Directory
3	Enable policy to block legacy authentication	+11.11%	0/8	To address	No	Yes	Identity	Azure Active Directory
4	Turn on sign-in risk policy	+9.72%	0/7	To address	No	Yes	Identity	Azure Active Directory
5	Turn on user risk policy	+9.72%	0/7	To address	No	Yes	Identity	Azure Active Directory
6	Do not allow users to grant consent to unmanaged applicatio...	+5.56%	0/4	To address	No	Yes	Identity	Azure Active Directory
7	Use Cloud App Security to detect anomalous behavior	+4.17%	0/3	To address	No	Yes	Apps	Microsoft Cloud App Security
8	Set automated notifications for new and trending cloud appli...	+4.17%	0/3	To address	No	Yes	Apps	Microsoft Cloud App Security
9	Restrict Anonymous user joins during meetings	+1.39%	0/1	To address	No	Yes	Apps	MS Teams
10	Discover trends in shadow IT application usage	+1.39%	0/1	To address	No	Yes	Apps	Microsoft Cloud App Security

Compliance Score

Compliance Score helps organizations manage compliance requirements. The Compliance Score is part of the Compliance Manager component within Microsoft 365.

Each Microsoft 365 Tenant receives an initial score based on data protection baselines. This baseline is a set of controls that includes crucial regulations and standards for data protection and general data governance. This baseline includes elements from NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) and ISO (International Organization for Standardization), as well as from FedRAMP (Federal Risk and Authorization Management Program) and GDPR (General Data Protection Regulation of the European Union).

Compliance Manager awards points for completing improvement actions taken to comply with a regulation, standard, or policy and combines those points into an overall compliance score. Each action has a different impact on your score, depending on the potential risks involved.

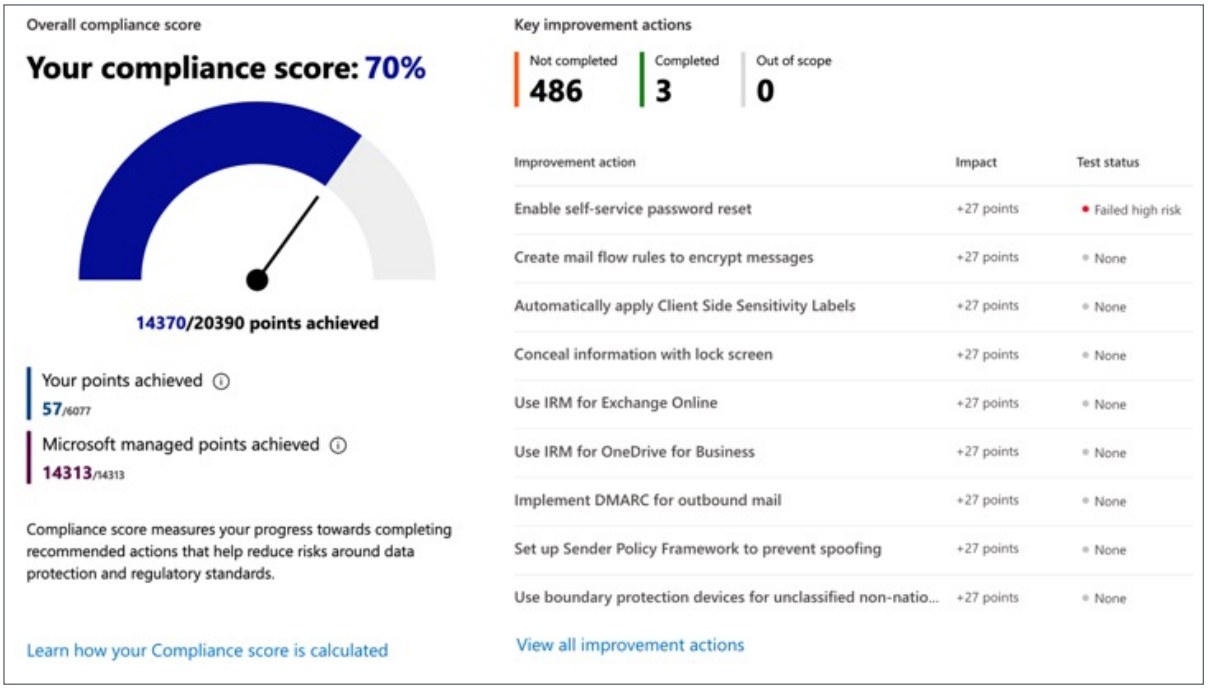
The compliance score is a calculation based on preventative, detected, and corrective actions or tasks. The score will change based on the organization's implementation of the recommended actions.

Compliance Manager

Compliance Manager helps to simplify compliance and reduce risk by providing four key features.

- Pre-built assessments for common industry and regional standards and regulations
- Workflow capabilities to help you efficiently complete any risk assessment
- Step-by-step guidance on suggested improvement actions
- Risk-based compliance score

Compliance Manager helps manage compliance with assessments for the regulations and certifications that apply to the organization. Assessments are logical groupings of controls from a specific regulation, standard, or policy.



Compliance Manager provides pre-built assessments that cover a variety of industry and regional regulations and certifications. Compliance Manager provides assessment templates to serve as a framework containing the necessary controls, improvement actions, and Microsoft actions for completing the assessment.

Additional Compliance Resources

As stated earlier, Microsoft is continually reviewing and updating the compliance standards and certifications provided through the Microsoft 365 platform. However, it is up to the customer to determine whether these standards satisfy your regulatory requirements. You can find the latest Microsoft certifications at https://servicetrust.microsoft.com/, including additional information on the following:

- Health Insurance Portability and Accountability Act (HIPAA)
- Data processing agreements (DPAs)
- Federal Information Security Management Act (FISMA)
- Federal Risk and Authorization Program (FedRAMP)
- ISO 27001
- European Union (EU) General Data Protection Regulation (GDPR)
- EU-U.S. Privacy Shield Framework
- Family Educational Rights and Privacy Act (FERPA)
- Statement on Standards for Attestation Engagements No. 16 (SSAE 16)
- Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)
- Gramm–Leach–Bliley Act (GLBA)

Governance Best Practices

Governance consists of the processes and procedures that an organization needs to follow to ensure that the users are being taken care of in a reasonable time frame and follow established security protocols and consistent processes. Consistency is the most significant thing regarding governance. It works best when everything is documented the same way, which helps define the return on investment (ROI) of the platform and a more vital ability to meet time frames and complete tasks when delivering andsupporting Office 365.

The first step to building a healthy governance strategy is always to sit down and discuss various organizational requirements and differences between teams and come to a shared understanding — before proposing any solution.

Microsoft's approach to governance in Microsoft 365 has been to invest in two primary areas: The Administration Console and expanded documentation through https://docs.microsoft.com/en-us/ office365/admin/admin-overview/

Managing a Microsoft 365 Tenant is not just about the technical configuration or deployment. A missing factor in most deployments is the continued management and control of the services and platform. Microsoft 365 provides governance and management tools either within the user interface or via the PowerShell command line.

Governance is not a single tool or dashboard, but is more focused on items such as change management, integration, and lifecycle management.

Overview of Governance Capabilities in Microsoft 365

Microsoft 365 provides many excellent governance capabilities. These features allow organizations to govern data for compliance or regulatory requirements.

The primary components are:

- Retention Policies and Labels
- Records Management
- eDiscovery and Legal Holds
- Auditing and Alert Policies

Each set of controls and policies allows organizations to meet many of the survey respondents' general governance concerns.

Retention Policies and Labels

For most organizations, the data volume and complexity of the data is increasing daily—email, documents, instant messages, and more. Effectively managing or governing this information is essential to comply proactively with industry regulations and internal policies, reduce risk in litigation or a security breach, and help the organization share knowledge effectively and be more agile.

When content has retention settings assigned to it, that content remains in its original location. Users can continue to work with their documents or mail as if nothing's changed. But if they edit or delete content included in the retention policy, a copy of the content is automatically retained.

Organizations can use both retention policies and retention labels with label policies to assign retention settings to content. Use a retention policy to assign the same retention settings for content at a site or mailbox level, and use a retention label to assign retention settings at an item level (folder, document, email). Retention labels are available for use with different types of content that require varying retention settings.

Records Management

All organizations types require a records-management solution to manage regulatory, legal, and business-critical records across their corporate data. Records management in Microsoft 365 helps to manage legal obligations, provide the ability to demonstrate compliance with regulations, and increase efficiency with the disposition of items no longer required.

Declaring content as records will enforce restrictions for allowing or blocking specific actions. Additionally, activities about the item get logged, so organizations have proof of disposition.

You use retention labels to mark content as a record or a regulatory record.

eDiscovery and Legal Holds

Electronic discovery, or eDiscovery, identifies and delivers electronic information as evidence in legal cases. eDiscovery tools allow searching for content within Exchange Online mailboxes, Microsoft 365 Groups, Microsoft Teams, SharePoint Online and OneDrive for Business sites, Skype for Business conversations, and Yammer teams.

Microsoft 365 provides the three eDiscovery tools: Content Search, Core eDiscovery, and Advanced eDiscovery.

Content Search

The Content Search tool within Microsoft 365 can find any email in Exchange mailboxes, documents in SharePoint sites and OneDrive locations, and instant messaging conversations in Skype for Business. Organizations can also use the content search tool to search for email, documents, and instant messaging discussions in collaboration tools such as Microsoft Teams and Microsoft 365 Groups. The identified results are then available to use within the Core and Advanced eDiscovery.

Core eDiscovery

Core eDiscovery in Microsoft 365 provides an essential eDiscovery tool that organizations can use to search and export content in Microsoft 365. It can also place content on eDiscovery hold within content locations, such as Exchange mailboxes, SharePoint sites, OneDrive accounts, and Microsoft Teams.

Advanced eDiscovery

Advanced eDiscovery in Microsoft 365 builds on the existing Microsoft eDiscovery and analytics capabilities. Advanced eDiscovery provides an end-to-end workflow to preserve, collect, analyze, review, analyze, and export content that's responsive to your organization's internal and external investigations.

Legal teams can manage the entire legal hold notification workflow to communicate with custodians involved in a case. Intelligent machine learning capabilities such as deep indexing, email threading, and near-duplicate detection also help you reduce large volumes of data to a relevant data set.

Auditing and Alert Policies

Microsoft 365 provides auditing capabilities for all types of actions, from end-user logins to application-specific tasks. All end-user and administration activities are available to search. All applications and services, including Azure Active Directory, provide log entries for searching and identification. All log entries are available for up to 90-days without using extra licensed retention policies.

Organizations can create alerts notifications such as emails for specific actions found within the audit log. These alerts allow administrators of the tenant to identify and manage more efficiently. Alert policies let administrators categorize the alerts triggered by a policy, apply the policy to all users in your organization, set a threshold level for when an alert is triggered, and then decide whether to receive email notifications when alerts are triggered.

Conclusion

For many years, the partner community – ISVs (independent software vendors), SIs (strategic integrators or consulting companies), and the MVP community – have provided content, tools, and expertise to help manage gaps in the platform. However, Microsoft has stepped up their game in this area, investing heavily in the platform's overall management experience and the documentation in support of the features and tools that they bring to market.

One of the hard lessons for many organizations, as with most user-driven technologies, is technology's deployment without proper planning or governance processes. As a result, many administrators find themselves in reactionary modes and quickly research and retroactively apply standards across their environment. Even the most proactive, process-oriented organizations struggle from time to time with managing governance across rapidly deployed collaboration platforms and services, many of which are being acquired and deployed without the IT team's prior knowledge or oversight.

A good governance strategy will outline how you intend to uphold policy and ensure your platform performs optimally. Healthy governance is essential to any successful platform. A strong governance strategy can directly impact end-user adoption and productivity, the level of management support received for current and future IT initiatives, and your ability to see the measurable business value.

Governance should be a priority no matter what tools or platform you deploy, but certainly should be at the forefront of any decisions to roll out company-wide social tools. The recommendation is to begin by clarifying and documenting your permissions, information architecture, templates, content types, taxonomy within each workload—and ownership of each—and then map those requirements to your platform roadmap. Define what policies, procedures, and metrics are necessary to manage your entire environment, and then look at what is possible across your many different tools and platforms.

About the Authors

Liam Cleary

Liam began his career as a Trainer of all things computer related. He quickly realized that programming, breaking, and hacking was a lot more fun. He spent the next few years working within core infrastructure and security services until he found SharePoint. He is the founder and owner of SharePlicity, a consulting company that focuses on all areas of Technology. His role within SharePlicity is to help organizations implement technology that will enhance internal and external collaboration, document and records management, automate business processes, and of course security controls and protection. He is also a Microsoft MVP and Microsoft Certified Trainer, focusing on Architecture but also crosses the boundary into Development. His specialty over the past few years has been security in SharePoint and its surrounding platforms. He can often be found at user groups or conferences speaking, offering advice, spending time in the community, teaching his kids how to code, raspberry PI programming, hacking the planet or building Lego robots, and you can reach him at www.helloitsliam.com and @helloitsliam

Christian Buckley

Christian is an award-winning product marketer and technology evangelist, and both a Microsoft Regional Director (RD) and Most Valuable Professional (MVP) in the office Apps & Services category. His almost 30-year tech career has included Chief Marketing Officer and Chief Evangelist for several leading SharePoint ISVs, and he was part of the Microsoft team that launched the hosted SharePoint platform in Office 365. He has worked with some of the world's largest technology companies to build and deploy social, collaboration, and supply chain solutions, and sold his first software startup to Rational Software in 2001. Co-author of books on both SharePoint and software configuration management (SCM), Christian is one of the most widely published names within the Microsoft ecosystem, and can be found online at www.buckleyplanet.com and @buckleyplanet

CONTACT US +1-650-968-4018 | 1350 W. Middlefield Rd., Mountain View, CA 94043, USA | www.egnyte.com

EGNYTE

Egnyte gives IT and business users one unified platform to manage, secure, and gain insight into business files, across Microsoft and non-Microsoft sources and applications. More than 16,000 businesses use Egnyte to supercharge their M365 deployment with seamless collaboration, strong access control, content governance and security for SharePoint, OneDrive, and Windows File Servers.