Microsoft Compliance Manager (preview)

07/02/2020 • 9 minutes to read • +7

In this article

> **Important**
>
> Compliance Manager isn't available in Office 365 operated by 21Vianet, Office 365 Germany, Office 365 U.S. Government Community High (GCC High), or Office 365 Department of Defense.

In this article: Read this article to learn what Compliance Manager is and understand its main components.

Learn about updates: Visit the Compliance Manager release notes to see what's new and known issues.

What is Compliance Manager

Microsoft Compliance Manager (preview) is a free workflow-based risk assessment tool in the Microsoft Service Trust Portal for managing regulatory compliance activities related to Microsoft cloud services. Part of your Microsoft 365, Office 365, or Azure

Active Directory subscription, Compliance Manager helps you manage regulatory compliance within the shared responsibility model for Microsoft cloud services.

With Compliance Manager, your organization can:

- Combine detailed compliance information Microsoft provided to auditors and regulators about its cloud services with your compliance self-assessment for standards and regulations applicable for your organization. These include standards and regulations outlined by the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST), the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), and many others.
- Enable you to assign, track, and record compliance and assessment-related activities, which can help your organization cross team barriers to achieve your compliance goals.
- Provide a Compliance Score to help you track your progress and prioritize auditing controls that help reduce your organization's exposure to risk.
- Provide a secure repository for you to upload and manage evidence and other artifacts related to your compliance activities.
- Produce richly detailed Microsoft Excel reports that document compliance activities performed by Microsoft and your organization for auditors, regulators, and other compliance reviewers.

> **Important**
>
> Recommendations from Compliance Score and Compliance Manager should not be interpreted as a guarantee of compliance. It is up to you to evaluate and validate the effectiveness of customer controls per your regulatory environment. These services are currently in preview and subject to the terms and conditions in the **Online Services Terms**. See also **Microsoft 365 licensing guidance for security and compliance**.

Relationship to Compliance Score

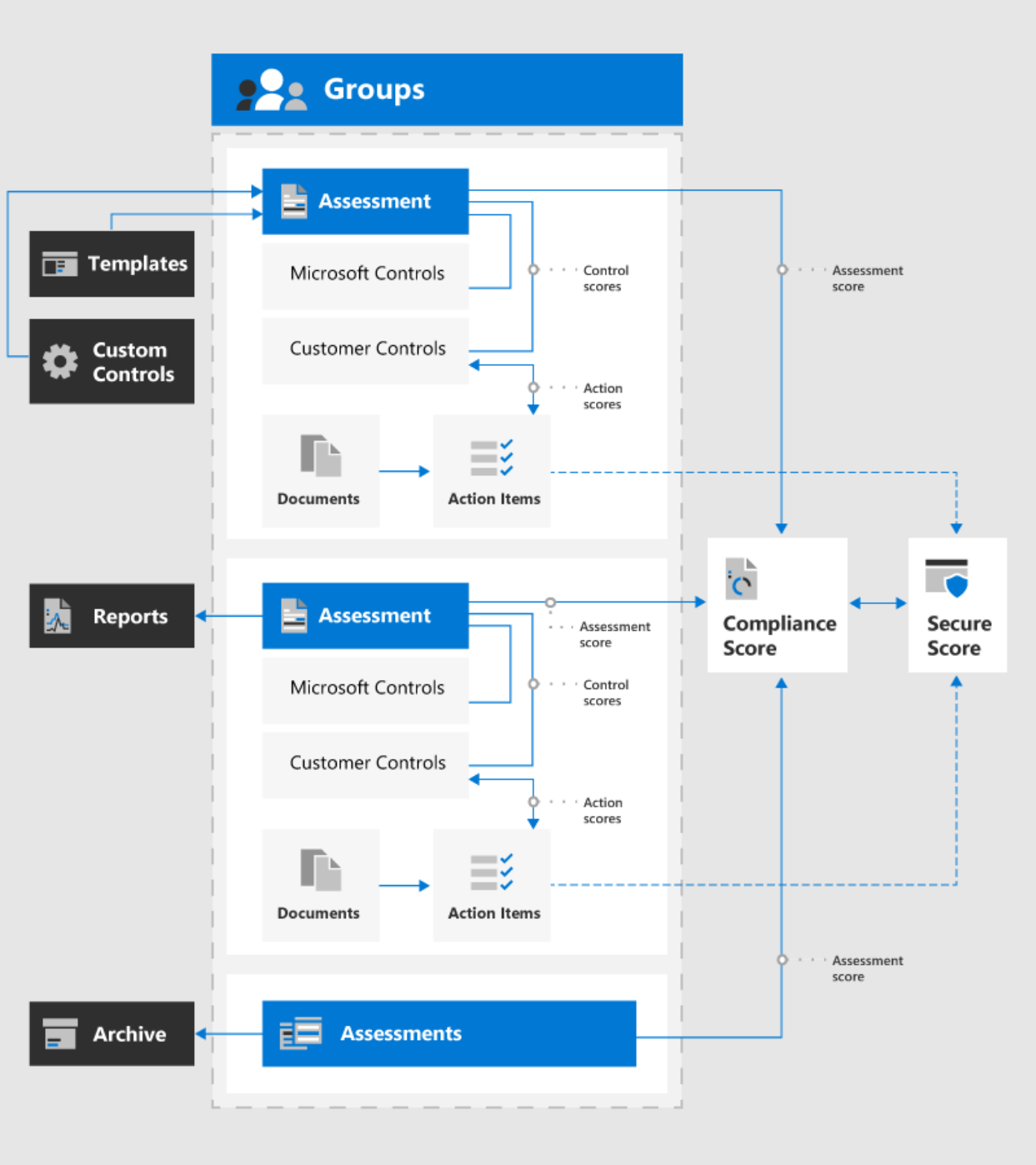
Microsoft Compliance Score (preview) is a feature in the Microsoft 365 compliance center that provides a top-level view into your organization's compliance posture. It calculates a risk-based score measuring your progress in completing actions that help reduce risks around data protection and regulatory standards. Knowing your overall compliance score helps your organization understand and manage compliance. Understand how your compliance score is calculated.

Compliance Manager shares the same backend with Compliance Score. During the public preview phase for both tools, Compliance Manager is where you'll manage your custom control implementations. Learn more about the relationship between Compliance Score and Compliance Manager.

Compliance Manager components

Compliance Manager uses several components to help you with your compliance management activities. These components work together to provide a complete management work flow and hassle-free compliance reports for auditors.

The diagram shows the relationships between the primary components of Compliance Manager:



Groups

Groups are containers that allow you to organize Assessments and share common information and workflow tasks between Assessments that have the same or related customer-managed controls. When two different Assessments in the same group share customer-managed control, the completion of implementation details, testing, and status for the control automatically synchronize to the same control in any other Assessment in the Group. This unifies the assigned Action Items for each control across the group and reduces duplicating work. You can also choose to use groups to organize. Assessments by year, area, compliance standard, or other groupings to help organize your compliance work.

Assessments

Assessments are containers that allow you to organize controls based on responsibilities shared between Microsoft and your organization for assessing cloud service security and compliance risks. Assessments help you implement data protection safeguards specified by a compliance standard and applicable data protection standards, regulations, or laws. They help you discern your data protection and compliance posture against the selected industry standard for the selected Microsoft cloud service. Assessments are completed by the implementation of controls included in the Assessment that map to a certification standard.

By default, Compliance Manager creates the following Assessments for your organization:

- Office 365 ISO 27001
- Office 365 NIST 800-53
- Office 365 GDPR

Assessments have several components:

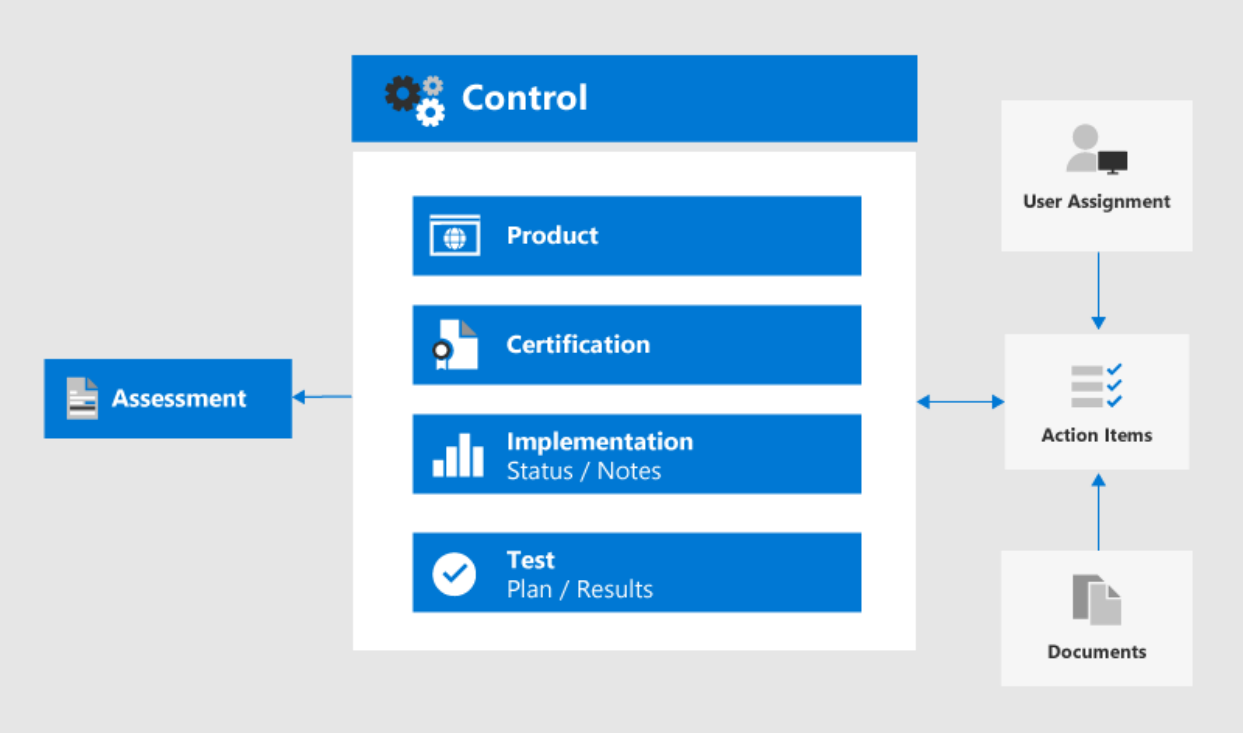
- **In-Scope Services**: Each assessment applies to a specific set of Microsoft services.
- **Microsoft-managed controls**: For each cloud service, Microsoft implements and manages a set of compliance controls for applicable standards and regulations.
- **Customer-managed controls**: These controls are implemented by your organization when you take actions for each control.
- **Assessment Score**: The percentage of the total possible score for customer-managed controls in the Assessment. This helps you track the implementation of the Actions assigned to each control.

Controls

Controls are compliance process containers in Compliance Manager that define how you manage compliance activities. These controls are organized into control families that align with the Assessment structure for corresponding certifications or regulations.

- **Control ID**: The name of the selected control from the corresponding certification or regulation.
- **Control Title**: The title for the Control ID from the corresponding certification or regulation.
- **Article ID**: This field is only for GDPR assessments and specifies the corresponding GDPR article number.

- **Description**: Text of control from the corresponding certification or regulation. Due to copyright restrictions, a link to relevant information is listed for ISO standards.



There are three types of controls in Compliance Manager, **Microsoft-managed controls**, **customer-managed controls**, and **Shared management controls**.

Microsoft-managed controls

For each cloud service, Microsoft implements and manages a set of controls as part of Microsoft's compliance with various standards and regulations. Each control provides details about how Microsoft implemented the control, and how and when that implementation was tested and validated by Microsoft and/or by an independent third-party auditor.

Customer-managed controls

Customer-managed controls are managed by your organization. Your organization is responsible for customer-managed control implementation as part of your compliance process for a given standard or regulation. Customer-managed controls are organized into control families for the corresponding certification or regulation. Use the customer-managed controls to implement the recommended actions suggested by Microsoft as part of your compliance activities. Your organization can use the prescriptive guidance and recommended customer actions in each customer-managed control to manage the implementation and assessment process for that control.

Customer-managed controls in Assessments also have built-in workflow management functionality that you can use to manage and track your progress towards Assessment completion. With this workflow functionality, you can:

- Assign Action Items for each control
- Track assigned Action Items
- Upload evidence of the implementation of the control
- Document the testing and validation of the control
- Mark the Action Items as implemented and tested

For example, a Compliance Officer in your organization assigns an Action Item to an IT admin with the responsibility and necessary permissions to perform the recommended action. The IT admin uploads evidence of the implementation tasks (screenshots of configuration or policy settings) and assigns the Action Item back to the Compliance Officer when completed. The Compliance Officer evaluates the collected evidence, tests the implementation of the control, and records the implementation date and test results in Compliance Manager.

Shared management controls

A shared control refers to any control where Microsoft and customers both share responsibilities for implementation. For example, controls related to personnel screening, account and password management, and encryption require actions by both Microsoft and customers.

Action Items

Actions Items are included in customer-managed controls as part of the built-in workflow management functionality that you can use to manage and track your progress towards Assessment completion.

People in your organization can use Compliance Manager to review the customer-managed controls from all Assessments for which they're assigned. When a user signs in to Compliance Manager and opens the **Action Items** dashboard, a list of Action Items assigned to them is displayed. Depending on the Compliance Manager role assigned to the user, they can provide implementation or test details, update the Status, or assign Action Items.

Certification controls are typically implemented by one person and tested by another. For example, after Action Items initially assigned to one person for implementation are completed, those Action Items are assigned to the next person to test and upload evidence. Any user with sufficient permissions for control assignments can assign and

reassign Action Items. This enables central management of control assignments and decentralized routing of Action Items between implementors and testers.

Note that **Improvement actions** in Compliance Score are the equivalent of **Action Items** in Compliance Manager.

Permissions

Compliance Manager uses a role-based access control permission model. Only users who are assigned a user role may access Compliance Manager, and the actions allowed by each user are restricted by role type. View a table showing the actions allowed for each permission.

The portal admin for Compliance Manager can set permissions for other users in within Compliance Manager by following these steps:

1. From the top **More** drop-down menu, select **Admin**, then **Settings**.
2. From here, select the role you want to assign, and then add the employee you want to assign to that role. Users will then be able to perform certain actions.

Users who are assigned the Global Reader role in Azure Active Directory (Azure AD) have read-only permission to access Compliance Manager. However, they cannot edit data or perform any actions within Compliance Manager.

There is no longer a default **Guest access** role. Each user must be assigned a role in order to access and work within Compliance Manager.

Manage evidence

Compliance Manager can store evidence of your implementation tasks around testing and validation of customer-managed controls. Evidence includes documents, spreadsheets, screenshots, images, scripts, script output files, and other files. Compliance Manager also automatically receives telemetry and creates an evidence record for Action Items that are integrated with Secure Score. Any data uploaded as evidence into Compliance Manager is stored in the United States on Microsoft Cloud Storage sites. This data is replicated across Azure regions located in Southeast Asia and Western Europe.

Templates

Compliance Manager provides pre-configured templates for Assessments and allows you to create customized templates for customer-managed controls for your compliance needs. New templates are created by importing controls information from an Excel file, or you can create a template from a copy of an existing template.

The pre-configured templates are:

1. Brazil General Data Protection Law (LGPD)
2. California Consumer Privacy Act (CCPA) (preview)
3. Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) 3.0.1
4. Dubai Information Security Resolution (DGISR)
5. European Union GDPR
6. Federal Financial Institutions Examination Council (FFIEC) Information Security Booklet
7. FedRAMP Moderate
8. HIPAA / HITECH
9. IRAP / Australian Government ISM (preview)
10. ISO 27001:2013
11. ISO 27018:2014
12. ISO 27701:2019
13. Microsoft 365 Data Protection Baseline
14. NIST 800-53 Rev. 4
15. NIST 800-171
16. NIST Cybersecurity Framework (CSF)
17. SOC 1
18. SOC 2

Secure Score integration

Compliance Manager is integrated with Microsoft Secure Score to automatically apply Secure Score credit to the Compliance Score for synced Action Items. This is configurable for individual Action Items or all actions globally, and provides updates from Secure Score.

For example, you have a security-related requirement for activating Azure Rights Management in your organization that also applies to a compliance-related Action Item. When Azure Rights Management is activated and processed by Secure Score, Compliance Manager receives notification of the update, and the score for the Action Item automatically updates with completion credit.

Ready to get started?

Start working with Compliance Manager to manage regulatory compliance activities for your organization.

Resources

- Interactive guide: Assess and enhance your data protection controls with Compliance Manager
- Microsoft Security, Privacy, and Compliance Tech Community

Is this page helpful?

Yes No