Simplify your compliance journey with Service Trust Portal and Compliance Manager
Table of contents

00. Executive summary
01. Compliance challenges
02. Microsoft control framework
03. Shared responsibilities: Microsoft and you
04. Service Trust Portal
05. Compliance Manager
06. Use scenarios: Service Trust Portal and Compliance Manager
07. Conclusion
Executive summary

Conducting risk assessments of information management systems is a critical activity for any organization. Many organizations must conduct annual risk assessments or audits to gain an understanding about the ongoing effectiveness of security, compliance, and privacy controls implemented by their organization or their cloud service provider. For regulated organizations that are considering or using a cloud service, you must perform due diligence to know if the cloud service meets your security, compliance, and privacy requirements.

In this document, we discuss some of the solutions from Microsoft that help customers to overcome the challenges that can make it difficult to achieve organizational compliance when using cloud services. These solutions provide you with rich details about Microsoft’s internal controls and how they are designed to meet comprehensive regulatory standards. For organizations that are considering or have just adopted Microsoft Cloud services, we explain the mechanism and the benefits of shared responsibilities of achieving compliance when using Microsoft Cloud services.

To help you overcome compliance management challenges, meet regulatory requirements, and conduct self-service audits and risk assessments, we’ve introduced the Service Trust Portal and Compliance Manager. They’re designed to help organizations meet complex compliance obligations and improve data protection capabilities when choosing and using Microsoft Cloud services.

Finally, we summarize various scenarios using the Service Trust Portal and Compliance Manager with highlighted resources. After reading this white paper, you’ll gain a deep understanding about how to use these tools to conduct self-service audits and risk assessments on Microsoft Cloud services.
Compliance challenges

Data protection compliance is a complex and disjointed process. To achieve organizational compliance, compliance personnel need to have a solid understanding of risk assessment, auditing, operations, technology, and more. However, it’s hard to find talent who have comprehensive knowledge in all these areas. Typically, compliance personnel are the experts in industrial regulations and standards, while IT professionals are the experts in technology solutions. It’s challenging to find talent with expertise in both areas to help define, implement, and assess controls. The disconnection between compliance and IT departments makes it challenging to equip an organization with enough capabilities to achieve data protection compliance.

Moreover, in this mobile-first, cloud-first world, organizations now encourage employees to use multiple devices and various on-premises or cloud applications to enhance their productivity. Multiple data-hosting assets further increase the complexity of data protection compliance.
According to the Cost of compliance 2017 report from Thomson Reuters authored by Stacey English and Susannah Hammond, there are more than 200 updates from 750 regulatory bodies every day from all over the world. It’s a big burden for compliance personnel to stay up-to-date with all the changes. Moreover, 32 percent of companies spend more than four hours per week merely creating and amending reports to the board.

This means compliance personnel need more assistance, either from a software service or consulting service, to help them meet evolving regulatory requirements. In Figure 1, we can see that heavy human involvement is invested in upfront policy interpretation and internal audits. Organizations need to have enough knowledge to interpret policies and define internal controls to meet requirements. They also need strong technology capabilities to implement data-protection-related controls, as well as a better way to manage all their compliance records for audits.

From the facts above, we know that achieving organizational compliance is extremely challenging. To help organizations manage compliance requirements from a single place, Microsoft developed a new solution, Compliance Manager. You can find more details below.

200 updates from 750 regulatory bodies every day from all over the world.
Microsoft control framework

In Microsoft, we demonstrate our cloud compliance to organizations transparently to build their trust in our cloud and to help them become more willing to adopt and use cloud technology. Obtaining compliance certification is one of the best ways to prove to businesses that we understand what is needed to protect their data. The certification process also motivates us to design better controls. Having a control framework helps Microsoft manage the compliance activities more efficiently because of common requirements from various regulations and standards.

1,900 controls that help to meet requirements of various regulations and standards
As shown in Figure 2, you can see that within one control set there are several controls helping to meet multiple regulatory requirements. For example, Control ID 3 and Control ID 4 help the business to meet the regulatory requirements of both Regulation A and Regulation B. Organizations just need to implement one control to meet two regulatory requirements. Microsoft has more than 1,900 controls that help to meet requirements of various regulations and standards, including GDPR, ISO 27001, ISO 27018, FedRAMP, HIPAA, and others. Having such a broad set of controls implemented and tested gives Microsoft the ability to support regulations and standards worldwide.
When organizations have their data on-premises, they are responsible for 100 percent of the controls to secure data and be compliant with regulations or standards.

Once they move their data to cloud services, such as Office 365, Dynamics 365, or Azure, it becomes a partnership—a shared responsibility—to achieve compliance (Figure 3). Microsoft assumes and manages the larger part of these controls for software as a service (SaaS) like Office 365, Dynamics 365, and others. This enables organizations to focus on and manage a smaller subset of data protection and regulatory compliance controls.

Microsoft manages the majority of the controls when organizations use SaaS applications like Office 365 and more.
Under this shared responsibility model, Microsoft is partnering with organizations to help them protect their data and stay compliant with relevant regulations and standards when they use Microsoft Cloud services. Let’s take the example of NIST 800-53: In the standard’s latest iteration, there are 1,021 controls. 79 percent of those controls are Microsoft’s responsibility, while only 21 percent are the customer’s responsibility.

Even more compelling is that Microsoft not only takes care of its own responsibilities, but also provides customers with tools and features to help them cover theirs (Figure 4). For example, with Office 365, we use Lockbox to restrict and control access to the production environment and customer data, but also offer features like Customer Lockbox, which allows customers to be part of the chain of approval required for elevated access. Another example is encryption, where we deliver baseline industry-standard encryption by default for...
data in transit and at rest, but also provide features like Azure Information Protection and Office 365 Customer Key to give customers additional levels of control. A final example is personnel control, where responsibility is equally shared. At Microsoft, we train our employees to protect customer data and report suspected security incidents, and we emphasize the need for customers to do the same in their organizations.
Microsoft is dedicated to building trust with organizations all over the world. The proof is in our commitment to protecting customers in a cloud-first world and our transparency about our operational details and best practices.

The Service Trust Portal is your go-to website for in-depth information and tools to help meet your security, compliance, and privacy needs when using Microsoft Cloud services, including Azure, Office 365, Dynamics 365, Intune, and Windows. The Service Trust Portal is a “one-stop shop” where we publish resources for performing self-service risk assessments of our cloud services, along with tools for tracking regulatory compliance activities within our cloud.

As a privacy officer, compliance officer, risk assessor, security officer, or legal officer, you’ll be able to find these resources on the website:
Track Compliance
Manage your organization’s regulatory compliance activities in the Microsoft Cloud

Audit Reports
See how the Microsoft Cloud complies with standards that matter to your organization

Data Protection
Get details on how the Microsoft Cloud is designed to protect customer data

Privacy
Learn about Microsoft capabilities that support your privacy and GDPR compliance obligations

Compliance Manager
This self-service risk assessment tool enables you to track, assign, and verify your organization’s compliance activities related to Microsoft Cloud services, such as Office 365, Dynamics 365, and Microsoft Azure. (You can find more details in the next section.)
Trust documents

Currently, there are three categories of documents that provide many resources for assessing Microsoft Cloud; learning our security, compliance, and privacy practices; and improving data protection capabilities.

Audit reports
Audit reports help you stay current on the latest privacy, security, and compliance information for Microsoft Cloud services. This includes ISO, SOC, FedRAMP, and other audit reports, bridge letters, and materials related to independent third-party audits of Microsoft Cloud services.

Data protection guides
Data protection guides provide information about how Microsoft Cloud services protect your data, and how you can manage cloud data security and compliance for your organization. This includes deep-dive white papers that provide details on the design and operation of our cloud services, FAQs, end-of-year security assessments, penetration test results, and compliance guide, which is the guidance for conducting risk assessments and improving data protection capabilities.

Azure Security and Compliance Blueprints
Azure Security and Compliance Blueprints provide resources to assist with building and launching cloud-powered applications that help organizations comply with regulations and standards. Blueprints include resources listed below for government, finance, healthcare, and retail industries:

- Industry-specific overview and guidance
- Customer responsibilities matrix
- Reference architectures with threat models
- Control implementation matrices
- Automation to deploy reference architectures
Privacy resources

Documentation and tools for data protection impact assessments, data subject requests (DSRs), and data breach notifications are provided to incorporate into your own accountability program in support of the General Data Protection Regulation (GDPR). The privacy section provides resources for multiple areas, including the following.

Data subject requests
DSRs provide information about how specific Microsoft Cloud services enable organizations to discover, access, rectify, restrict, delete, and export personal data, and how they connect organizations to the DSRs tools Microsoft builds to help them respond to DSRs (for example, Data Log Export for responding to telemetry log DSRs).

Data breach notifications
Data breach notifications provide information about how Microsoft detects and responds to personal data breaches, and how organizations can set up their privacy contact to receive breach notifications from Microsoft in the event of a personal data breach.

Data protection impact assessments
Data protection impact assessments provide information about Microsoft’s and organizations’ responsibilities for DPIA compliance, and documentation from Microsoft that can support organizations to create their own DPIAs on Microsoft Cloud services.

Other resources
In addition to the tools and guidance discussed above, the Service Trust Portal provides other compliance-related resources, including guidelines for regional compliance for different regions (such as the Czech Republic, Poland, and Romania); additional materials for the Security and Compliance Center; and frequently asked questions about the Service Trust Portal, Compliance Manager, and GDPR.

We will keep adding and updating the information for each offering in the Service Trust Portal, with the goal of providing a similar experience across all Microsoft Cloud services.
Compliance Manager

Key capabilities

**Compliance Manager** enables you to manage your organization’s compliance activities from one place. It’s a cross-Microsoft-Cloud solution that helps organizations understand and manage the complex compliance landscape. It enables organizations to perform ongoing risk assessments with Compliance Score, provides actionable insights that help to improve data protection capabilities, and simplifies processes with the built-in collaboration and audit-ready reporting tools.

*Note:* Compliance Manager is a dashboard that provides the Compliance Score and a summary of your data protection and compliance stature as well as recommendations to improve data protection and compliance. This is a recommendation—it’s up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a guarantee of compliance.
As shown in Figure 6, Compliance Manager provides three key capabilities:

<table>
<thead>
<tr>
<th>Ongoing risk assessment</th>
<th>Actionable insights</th>
<th>Simplified compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get an intelligent score that reflects your current compliance posture</td>
<td>Get detailed information to assess the controls managed by Microsoft</td>
<td>Improve collaboration and streamline workflow with the control management tool</td>
</tr>
<tr>
<td>Available for Office 365, Azure, and Dynamics 365. Covers various standards and regulations such as GDPR, ISO 27001, ISO 27018, NIST 800-53 and more.</td>
<td>Get recommended actions to improve your data protection capabilities</td>
<td>Save time creating and amending reports for auditing activities</td>
</tr>
</tbody>
</table>

Figure 6: Key capabilities of Compliance Manager

**Ongoing risk assessment**
To help you assess Microsoft Cloud under the shared responsibility model, Compliance Manager provides a dashboard view of assessments that clearly shows you the implementation progress of controls that are under Microsoft’s responsibility and your organization’s responsibility. Compliance Manager enables your organization to perform ongoing risk assessments with a Compliance Score in each regulation or standard assessment. With this risk-based score, you can gain visibility into the compliance risks for each control managed by Microsoft and your organizations and perform a holistic risk assessment on your usage of Microsoft Cloud. The higher the score, the more compliant your usage of the cloud service is. Compliance Score also helps organizations make better control
implementation plans by prioritizing the controls with higher scores for immediate implementation and testing. For more on Compliance Score, see the callout page below.

**Actionable insights**
Compliance Manager provides rich insights into both Microsoft’s and your responsibilities for meeting compliance standards.

For controls that are identified as Microsoft’s responsibility, you can see the detailed information of our internal controls, including control implementation details, test plans, and test results that Microsoft provides to auditors and regulators as part of third-party audits (such as ISO 27001 audit). For controls with findings, Microsoft provides detailed management responses to help you understand the risk involved with those controls. We share this information because we are committed to being transparent about how we process and protect your data so that you can trust Microsoft and take advantage of the technology we provide.

For the controls that you manage, Compliance Manager enables you to conduct self-assessments to continuously monitor compliance performance. Implementing and passing the test of your internal controls can increase your Compliance Score. Compliance Manager not only helps you define controls and map them to corresponding regulatory requirements, but also provides recommended actions you can take to improve your data protection capabilities to meet those requirements.

**We help you make the connections that make cloud compliance an easier process.**

Within the recommended actions, we connect you to supporting documents that provide step-by-step guidance on how to configure or enable the security and compliance features. With Compliance Manager, you can find abundant resources that can help you achieve organizational compliance, including the security and compliance solutions in the Office Security and Compliance Center, Azure Security Center, and more. This means you don’t need to visit multiple platforms and search for the resources by yourself. We help you make the connections that make cloud compliance an easier process.
**Compliance Score**

Compliance Score is a risk-based score that assists you in conducting self-assessments for your regulatory responsibilities. A Compliance Score is assigned to each control based on the level of risks involved due to non-compliance or control failure. On the dashboard, Compliance Manager displays a total score for each assessment in the upper right-hand corner of the tile. This overall score is the accumulation of points received for each control that has been implemented and tested to date in the assessment. When you add an assessment for the first time, you’ll see that the Compliance Score is already a fraction of the way toward completion because the points for the Microsoft-managed controls are already applied. This is because those controls have been successfully implemented and tested. The remaining points come from successful customer control assessments—from the implementation and testing of customer-managed controls, each of which has a specific value that contributes to the overall Compliance Score.

---

**Default Group**

**Office 365 - GDPR**

**Actions**

- Created: 3/26/2018
- Modified: 4/6/2018

- Customer Managed Actions: 0 of 61
- Microsoft Managed Actions: 48 of 48

**Compliance Score**

- 243 of 568

**Default Group**

**Office 365 - NIST 800-53**

**Actions**

- Created: 3/26/2018
- Modified: 4/6/2018

- Customer Managed Actions: 0 of 215
- Microsoft Managed Actions: 760 of 760

**Compliance Score**

- 417 of 562
Based on the risk essence of the control, each control is assigned a possible number of points (called a severity ranking) on a scale from 1 to 10, where more points are awarded for controls associated with a higher risk factor if the control is not implemented or fails. After you implement and test a control, the organization can avoid the risk involved for the control, and the Compliance Score of the assessment increases by the number of points of that control. For example, the User Access Management control shown below has a very high severity ranking and displays an assigned value of 10. Once you implement this control, the Compliance Score of the GDPR assessment will increase by 10 points.

Follow these links for more information on how you can use the Compliance Score to meet your regulatory requirements on the Microsoft Cloud:

- [Understanding the Compliance Score](#)
- [Simplify your compliance journey with Compliance Manager](#)

### Simplified compliance

Compliance Manager helps to simplify the compliance process by providing you built-in tools to collaborate and track your compliance activities, reducing the need to rely on paperwork or spreadsheets to manually collect information across multiple teams.

To make it easier for collaboration across teams, the control management tool allows compliance officers and data protection officers to track each control in Compliance Manager and assign it to corresponding roles (such as IT admin, HR, or privacy team). The people assigned the task can enter the control implementation details and upload evidence to Compliance Manager to record their actions for auditing. Any data uploaded and stored in Compliance Manager is also stored in Microsoft Cloud storage, which is compliant with the

<table>
<thead>
<tr>
<th>Controls / Articles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control ID:</strong> 6.5.2</td>
</tr>
<tr>
<td><strong>Title:</strong> User access management</td>
</tr>
<tr>
<td><strong>Article ID:</strong> Article (5)(1)(f)</td>
</tr>
<tr>
<td><strong>Description:</strong> Article (5)(1)(f): Personal data shall be: (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (&quot;integrity and confidentiality&quot;).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Compliance Score</th>
<th>Related Controls / Articles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>10</strong></td>
<td>NIST 800-53: AC-2</td>
</tr>
</tbody>
</table>
data protection standards in Tier C of our Compliance Framework for Industry Standards. Tracking control progress in real-time across various workflows, compliance officers and risk assessors can perform proactive ongoing assessments to get ready for audits. You can generate richly detailed reports in a few clicks in Microsoft Excel to document Microsoft’s and your compliance activities, complete with links to the evidence collected. The audit-ready report can help your organization be better prepared for internal or external auditing; it also can be provided to auditors, regulators, and other compliance stakeholders.

To meet your auditing needs based on your organizational structure, Compliance Manager provides a Group functionality to help you group assessments by region, business unit, or year, depending on your compliance workload design. Records and evidence of common controls across regulations and standards in the same Group are synchronized, thereby reducing duplicated effort to satisfy identical requirements across different assessments.

For example, after you implemented control ID: 6.11.1 in GDPR assessment, eight other related controls in ISO, HIPAA, and NIST assessments would also get implemented with the same implementation and test details you entered in Compliance Manager.

Scope of Compliance Manager

Currently, Compliance Manager supports industrial standards such as International Organization for Standardization (ISO) 27001:2013, ISO 27018:2014, National Institute of Standards and Technology (NIST) 800-53, and NIST 800-171 and more. It also supports regulations such as the EU General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) and more. Note that the coverage of regulations and standards varies by cloud service (Azure, Dynamics 365, and Office 365). We will keep adding and updating the information for each cloud service, and our goal is to provide a similar user experience across all Microsoft Cloud services.
Compliance Manager has been launched as an additional value for Azure, Dynamics 365, and Office 365 Business and Enterprise customers in public clouds. Office 365 Government Community Cloud (GCC) customers can access Compliance Manager; however, organizations should evaluate whether to use the Document Upload feature of Compliance Manager, as the storage for document upload is compliant with Office 365 Tier C only. Compliance Manager is not yet available in sovereign clouds, including the United States Department of Defense (DoD), Office 365 operated by 21 Vianet, and Office 365 Germany.

**Roles in Compliance Manager**

By default, everyone in your organization with an Office 365 or Azure Active Directory account has access to Compliance Manager and can perform almost any action in it. The target audience for Compliance Manager is those individuals in your organization who are responsible for:

- Compliance
- Privacy
- Security
- Risk assessments
- Auditing
- Data protection
- IT administration

These users might already have a variety of Azure Active Directory administrator roles assigned to them, such as:

- Global administrator
- Exchange administrator
- Skype for Business administrator
- SharePoint administrator
- Compliance administrator
- Security administrator
- Several others

To control who has access to Compliance Manager—along with the level of access—using built-in Role Based Access Control (RBAC) for permissions, you must change the default permissions and configure Compliance Manager to be accessible to a limited set of users by adding at least one user to each Compliance Manager role (see these instructions).

After a user has been added to each role, the default permissions are removed and only users who’ve been added to a role will be able to access Compliance Manager and perform the actions allowed by that role.
For example, if you add a user to the role that lets users manage Assessments, only members of that role can manage Assessments. Similarly, if you don’t add a user to the role that lets users read the data in Assessments, then all users in your organization can access Compliance Manager and read data in any Assessment.

Table 1 describes each Compliance Manager permission role and what it allows the users do. The table also indicates the role that each permission is assigned to.

### Set up roles through Role-Based Access Control

<table>
<thead>
<tr>
<th>Permission</th>
<th>Guest</th>
<th>Reader</th>
<th>Contributor</th>
<th>Assessor</th>
<th>Administrator</th>
<th>Portal Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Read info provided by MS</strong></td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
<tr>
<td>Users can only read information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>provided by Microsoft, no tenant-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>specific info</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Read data</strong></td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
<tr>
<td>Users can read but not edit data.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Edit data</strong></td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
<tr>
<td>Users can edit all fields, except</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>the Test Result and Test Date</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fields.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Edit test result</strong></td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
<tr>
<td>Users can edit the Test Result</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>and Test Date fields.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Manage assessments</strong></td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td></td>
<td>⬜</td>
</tr>
<tr>
<td>Users can create, archive, and</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>delete Assessments.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Manage users</strong></td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td></td>
<td>⬜</td>
</tr>
<tr>
<td>Users can add other users in their</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>organization to the Reader,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contributor, Assessor, and</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrator roles.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Compliance Manager permission roles

*Only those users with the Global Administrator role can add or remove users from the Portal Admin role.*
Due diligence for Microsoft Cloud services

Before making the decision to use Microsoft Cloud services, your organization needs to conduct due diligence to ensure that the service supports its security and compliance needs. Here are some actions you can take:

- Gain more understanding about what certifications each Microsoft Cloud service has on the Compliance Offerings page on the Microsoft Trust Center. By using the filters on the page and clicking the certification, you can find relevant audit information.
• Create a trial account and log in to the Service Trust Portal to find all certifications, audit reports, security and compliance white papers, pen test reports, and more.

• Use your trial account to access Compliance Manager on the Service Trust Portal. Then, find the control implementation details for each cloud service and evaluate the solutions we provide to enhance your data protection capabilities.

Protect data in the cloud

As a security officer or data protection officer in your organization, you need to understand how to help protect data in the cloud and be compliant with the necessary regulatory requirements. Here are some steps you can take:

• Start by reading Better protect your data by using Microsoft Cloud services on the Trust Center.

• Find in-depth information about security, data protection, and security architecture from FAQs and white papers on the Service Trust portal. You can start by reading GDPR—Get organized and implement the right processes to better understand how you can start to act on meeting the regulatory obligations, as well as Microsoft Cloud—Encryption to learn about the various encryption features and technologies currently available for Microsoft Cloud services.

• Use Compliance Manager, starting with the GDPR assessment tile, to manage compliance-related activities. It can help connect the GDPR articles with data protection capabilities you can use to implement controls for meeting regulatory requirements. You can design your own business processes or statements of procedures (SOPs), if necessary, and record all details and evidence on this platform for further risk assessment and auditing.
Self-service audits

As a compliance officer or privacy officer, you’ll want to perform risk assessments on Microsoft Cloud services when your organization conducts annual audits or reviews these services during contract renewal. Here are some actions you can take on the Service Trust Portal to perform self-service audits:

• Visit the Audit Reports page to find all our audit reports and certificates for ISO, SOC, FedRAMP, and others across Microsoft Cloud services (including Azure, Office 365, Dynamics 365, and Windows).

• Use Compliance Manager to learn more about Microsoft controls and those managed by your organization. The dashboard shows a clear view of your compliance posture across Microsoft Cloud services, with various regulations and standards that matter to your organization. We’ve provided the most updated information about the Microsoft-managed controls on the dashboard, so you don’t need to download multiple reports to get the information you need for self-service audits.

• Take advantage of Microsoft guidance about how your organization can implement controls to gain compliance. With Compliance Manager, you can continuously conduct risk assessment on Microsoft-managed controls and do self-assessment on controls managed by your organization—and obtain richly detailed reports in preparation for internal and external auditing.
Conclusion

The Service Trust Portal and Compliance Manager help to simplify your compliance journey by giving you the information and tools to conduct risk assessment and manage your end-to-end compliance processes when using Microsoft Cloud services. You’ll be able to assess your compliance risks more easily with these two tools across the process of considering and adopting Microsoft Cloud services.

Contact Sales

© 2018 Microsoft Corporation. All rights reserved. This document is provided “as-is.” Information and views expressed in this document, including URL and other internet website references, may change without notice. You bear the risk of using it.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Compliance Manager is a dashboard that provides the Compliance Score and a summary of your data protection and compliance stature as well as recommendations to improve data protection and compliance. This is a recommendation—it is up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a guarantee of compliance.