Microsoft 365

Simplify compliance and reduce risk with Microsoft Compliance Score

Table of contents

Executive summary

Who this is for:

Companies who are looking for guidance to manage risk and compliance in the cloud.

Quick read:

With data growing at an exponential rate and the increasing number of data protection regulations, companies need better tools and more knowledge to assess and manage IT-related risk. Moving to the cloud can relieve some of the burden by making many requirements the responsibility of the vendor.

Microsoft is committed to helping simplify compliance through a trusted platform and tools such as Microsoft Compliance Score. This risk-based score helps measure how well your controls meet specific compliance standards and suggests actions to improve them.

Compliance challenges

The technological, operational, and regulatory complexity of compliance presents unique challenges.

> Being there are multiple categories of compliance, this is never simple … for any company servicing multiple industry sectors considering overlap, regulations, and incompatibilities between some compliance areas.”

Information Security Director[1]

> IT compliance as a skill set is relatively rare. Folks that have been dedicated or focused on this are hard to come by. It’s just a tough place to find good people.”

Enterprise Chief Information Security Officer[2]

[1, 2] "Microsoft customer research"

Keeping up with new and frequently updated regulations is an ongoing struggle

On average, there are 220 updates per day from 1,000 regulatory bodies. The rapid pace of change is one of the biggest compliance challenges organizations face, requiring them to live in a state of reaction.

Collaboration on risk and compliance management is inefficient and siloed

Unfortunately, IT and compliance teams don’t always understand each other. The IT side understands the technology, but lacks specialized knowledge required to interpret regulations. On the other hand, compliance and privacy teams know the rules very well, but are not experts in solutions that can help to meet the requirements.

Point-in-time assessments fail to identify risks between audits

Manual audits quickly go out of date, creating risks between assessments. Companies are looking for ways to integrate across systems better and keep assessments up to date in real time to match the digital pace of change.

Guidance is lacking to help with designing and implementing effective controls

IT decision-makers are overwhelmed with tools and technologies. They need simple, step-by-step guidance on how to make the tools work for their industry and their regulations.

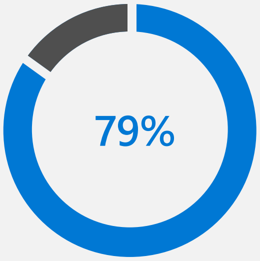
Simplify your compliance journey with help from this collection of guides, insights, and resources.

[3] "The Cost of Compliance," Reuters, 2019.

Shared responsibilities: Microsoft and you

Creating and maintaining data protection controls can be time-consuming and labor-intensive. If you keep all your data on-premises, you're solely responsible for compliance controls and managing the complexity that comes with them. When you use cloud services, compliance becomes a shared responsibility. With a trusted partner, this can significantly reduce the burden on your team.

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.



of those controls are Microsoft’s responsibility

Microsoft assumes and manages most of these controls for software as a service (SaaS) applications such as Microsoft 365. This frees you to focus on fewer controls so you can spend more time on strategic initiatives. Under this model, Microsoft partners with you to protect your data and simplify compliance. For example, consider NIST 800-53, which includes 1,021 controls. When you use Office 365, we handle almost 80 percent of them.

We also provide you with solutions to help manage your compliance responsibilities. For example, with Office 365, we not only use the Lockbox system to restrict and control access to the production environment and customer data, but also provide you with solutions like Azure Active Directory Conditional Access to help you build up effective access controls from your end.

Encryption is another area where we can make things easier. With Microsoft cloud services, we encrypt data in transit and at rest by default, and offer you Microsoft Information Protection and Customer Key to give you additional encryption control.

Shared responsibility is only valuable if you can trust the cloud service provider and have easy access to assess its controls. Microsoft introduced Microsoft Compliance Score, a risk-based score that allows you to easily assess Microsoft-managed controls, so you have full visibility into how Microsoft protects your data. In addition, the score provides you with recommended actions to implement and enhance your data protection controls.

Learn more about the shared responsibility model in the "Shared Responsibility for Cloud Computing" white paper.

Overview of Compliance Score

Microsoft Compliance Score helps you understand your organization's compliance posture. It measures your progress in completing actions that help reduce risks related to data protection and regulatory compliance. You can easily see your current score, areas for improvement, and actions to take.

Even if you're not an expert in complex regulations like GDPR, you can still quickly learn the actions recommended to help you progress toward compliance. With the ongoing control assessment, you can now proactively maintain compliance, instead of reactively fixing settings following an audit.

Continuously assess your risk

Eighty-eight percent of organizations are looking for tools to help them detect risk automatically, since point-in-time assessments can easily expose organizations to unidentified risks between periodic assessments like annual audits.[4]

Microsoft Compliance Score helps you identify risk continuously. It automatically scans your Microsoft 365 environments to detect and monitor the effectiveness of data protection controls in your system and alert you to potential risks.

For example, if your organization hasn't set up compliance policies for Windows devices, Compliance Score will highlight this control as failed with high risk and recommend that you add a device compliance policy in Intune. Once you add the policy, your score will be updated in 24 hours.

Get actionable recommendations

With so many regulations and technologies to keep track of, knowing what to do next to improve compliance can be challenging. Compliance Score recommends improvement actions aligned with data protection regulations and standards, and provides detailed implementation guidance, which helps compliance and IT teams to be on the same page.

The Compliance Score dashboard shows your improvement actions—the ones that address the most important issues and will increase your score by the largest number of points. You can easily assign actions to stakeholders in your organization to implement and test controls. On each action page, you can also upload and store evidence, as well as record implementation and test details to prepare for audits.

[4] Risk Management market landscape web survey (n=500, buyers and influencers of IRM solutions, 1000+ employees), Gartner, 2019.

Simplify compliance

Gartner has predicted that by 2022, half of the planet's population will have its personal information covered under local privacy regulations in line with the General Data Protection Regulation (GDPR), up from one-tenth today. IT decision makers describe the increasing number of regulations as trying to play "Whack-A-Mole" at a county fair: they are constantly reacting to change, rather than proactively addressing it.

At Microsoft, we've built a common control framework with 1,900 controls for our own services. It allows us to scale our assurance effort to meet compliance requirements from more than 90 regulations and standards. Using the same methodology, we shared the knowledge and built the common control framework in Microsoft Compliance Score, so you can leverage the built-in control mapping to scale your compliance effort. By taking one action, you can help your organization satisfy multiple requirements at the same time. It helps reduce time spent managing compliance and simplifies auditing by eliminating duplicate effort.

Learn more about Compliance Score.

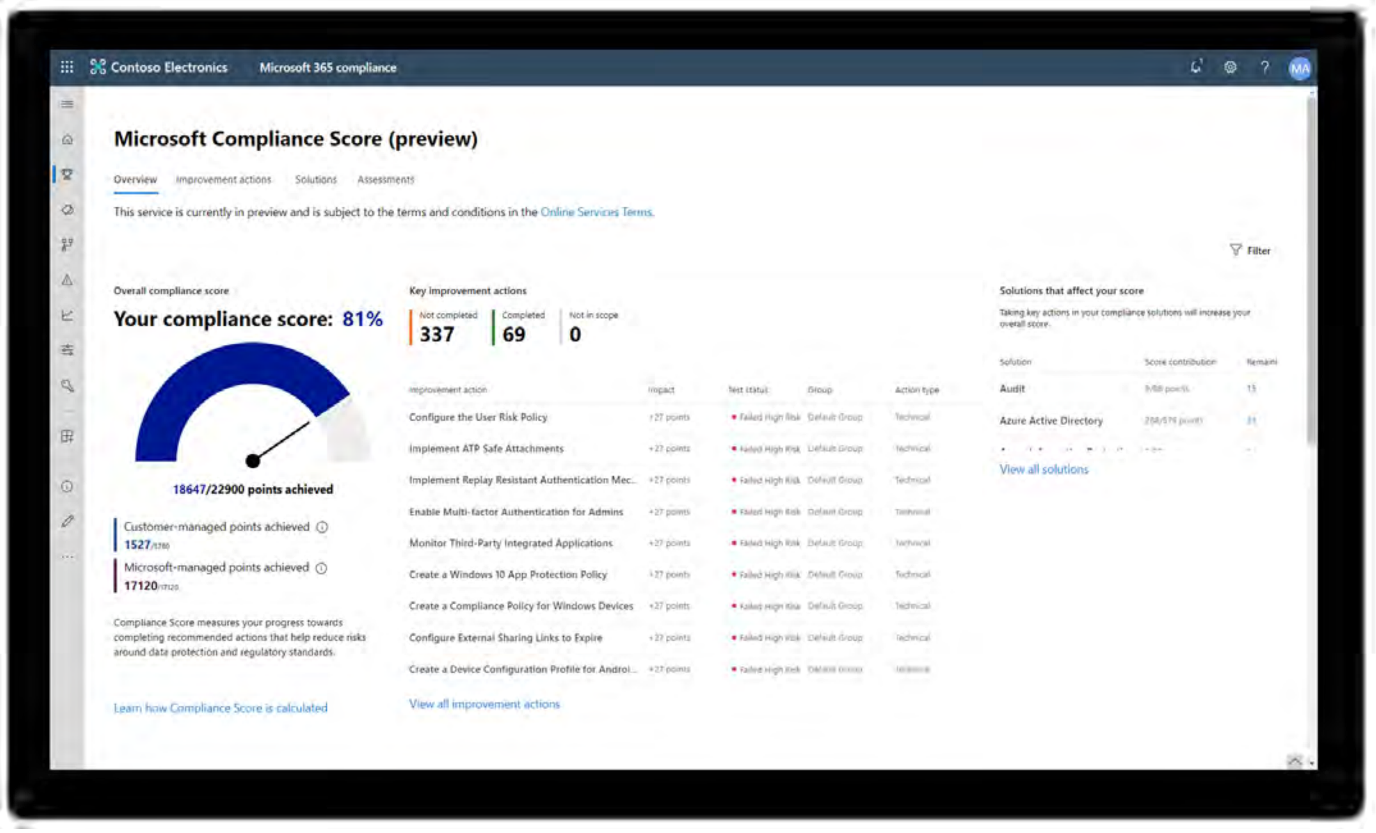
[5] "The state of privacy and personal data regulation," Nader Henein and Bart Willemsen, April 2019.

Understanding your score

Compliance Score provides an initial rating based on a data protection baseline composed of requirements from key global regulations and standards. You can then add specific assessments that are relevant to your organization. For example, a bank might want to add the FFIEC assessment. Or if you work for a hospital, you can add the HIPAA/ HITECH assessment.

Most of the points come from Microsoft-managed controls because of the shared responsibility model described earlier in this white paper. Aspects available to you to improve are listed as customer-managed points. When you take actions and implement controls, you will see the compliance score increase accordingly.

You can see a breakdown of contributions to your score by category, such as information protection and access control. The score category helps you focus on the areas that need the most attention and assign to the right admins to help you with the actions.



Microsoft Compliance Score (preview)

This service is currently in preview and is subject to the terms and conditions in the Online Services Terms.

Overall compliance score

Your compliance score: 81%

18647/22900 points achieved

Customer-managed points achieved
1527/5780

Microsoft-managed points achieved
17120/17120

Compliance Score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Learn how Compliance Score is calculated

Key improvement actions

Not completed	Completed	Not in scope
337	69	0

Improvement action	Impact	Test status	Group	Action type
Configure the User Risk Policy	+27 points	● Failed High Risk	Default Group	Technical
Implement ATP Safe Attachments	+27 points	● Failed High Risk	Default Group	Technical
Implement Replay Resistant Authentication Mec...	+27 points	● Failed High Risk	Default Group	Technical
Enable Multi-factor Authentication for Admins	+27 points	● Failed High Risk	Default Group	Technical
Monitor Third-Party Integrated Applications	+27 points	● Failed High Risk	Default Group	Technical
Create a Windows 10 App Protection Policy	+27 points	● Failed High Risk	Default Group	Technical
Create a Compliance Policy for Windows Devices	+27 points	● Failed High Risk	Default Group	Technical
Configure External Sharing Links to Expire	+27 points	● Failed High Risk	Default Group	Technical
Create a Device Configuration Profile for Androi...	+27 points	● Failed High Risk	[illegible]	[illegible]

View all improvement actions

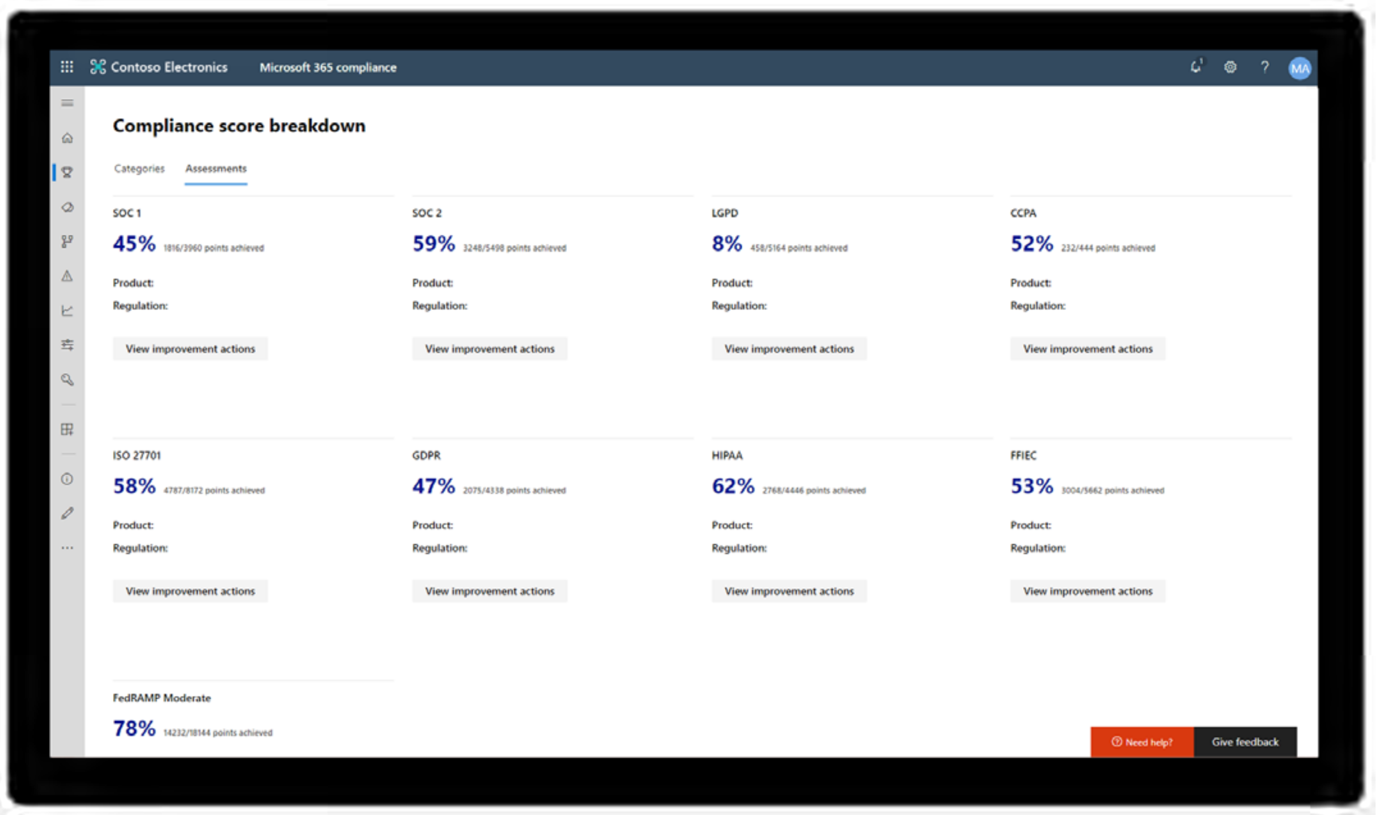
Solutions that affect your score

Taking key actions in your compliance solutions will increase your overall score.

Solution	Score contribution	Remaini
Audit	[illegible] points	15
Azure Active Directory	[illegible] points	[illegible]
[illegible]	[illegible]	[illegible]

View all solutions

You can also see the score breakdown by regulations and standards you selected, which is especially useful for your compliance and risk assessment teams. IT admins can also easily understand what actions can help improve the score and how they contribute to overall compliance goals.



Compliance score breakdown

SOC 1
45% 1816/3960 points achieved
Product:
Regulation:

SOC 2
59% 3248/5498 points achieved
Product:
Regulation:

LGPD
8% 458/5164 points achieved
Product:
Regulation:

CCPA
52% 232/444 points achieved
Product:
Regulation:

ISO 27701
58% 4787/8172 points achieved
Product:
Regulation:

GDPR
47% 2075/4338 points achieved
Product:
Regulation:

HIPAA
62% 2768/4446 points achieved
Product:
Regulation:

FFIEC
53% 3004/5662 points achieved
Product:
Regulation:

FedRAMP Moderate
78% 14232/18144 points achieved

Figure 1. Score breakdown by category helps you identify categories that need more immediate attention.

Get started

As the pace of digital transformation increases, managing risk can't be a once-a-year activity. Microsoft Compliance Score empowers you to continuously monitor the effectiveness of your controls based on your specific regulatory environment. It empowers various teams, including IT, security, and more, in your organization to understand and make improvements to compliance. A common control framework increases efficiency, while built-in workflow tools enable effective collaboration. It's your go-to tool for reducing risk and managing compliance complexity.

You can sign up for a trial or navigate to the Microsoft 365 compliance center to get started today. You can learn more about Microsoft Compliance Score in this supporting document.

Contact us

Note: Compliance Score is a risk-based score that helps you simplify and automate risk assessments and provides recommendations to help you address risks. It does not express an absolute measure of organizational compliance with any particular standard or regulation. It expresses the extent to which you have adopted controls which can reduce the risks to personal data and individual privacy. Compliance Score should not be interpreted as a guarantee in any way.

Microsoft 365