



## Lab 1 - Compliance Manager

This lab contains five activities. These are shown below:

- [Part 1 – Compliance Manager](#)
- [Part 2 – Compliance Assessments](#)
- [Part 3 – Make your own Compliance template](#)
- [Part 4 – Overview of Trust Documents](#)
- Part 5 – Extensions
  - [Extension a – Secure Score Planner integration](#)
  - [Extension b – Service Now Intergration](#)

### Pre-requisites

Before you start you should have completed the “Getting started with Microsoft 365 Compliance Master Class Labs”. If you have not completed this you will not be able to do this lab. You can find this document which you can download from <https://aka.ms/m365masterclass-Intro>. Each tenant will take 24 hours to provision so its important that you complete this prior to Tuesday when the event starts.

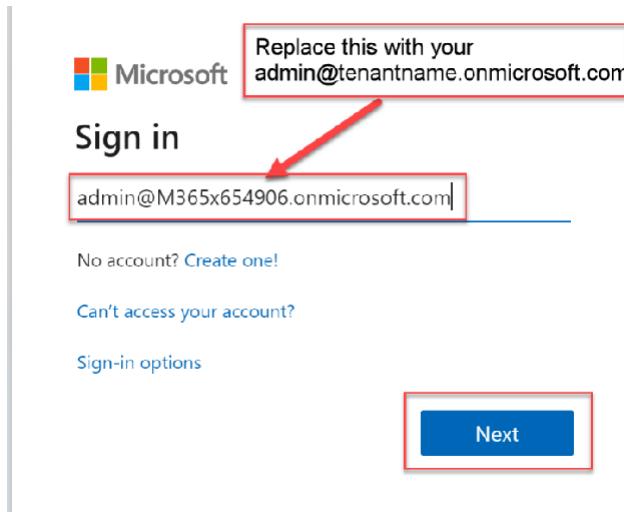
### Part 1 - Compliance Manager

**Microsoft Compliance Score is a preview feature in the Microsoft 365 compliance center to help you understand 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.**

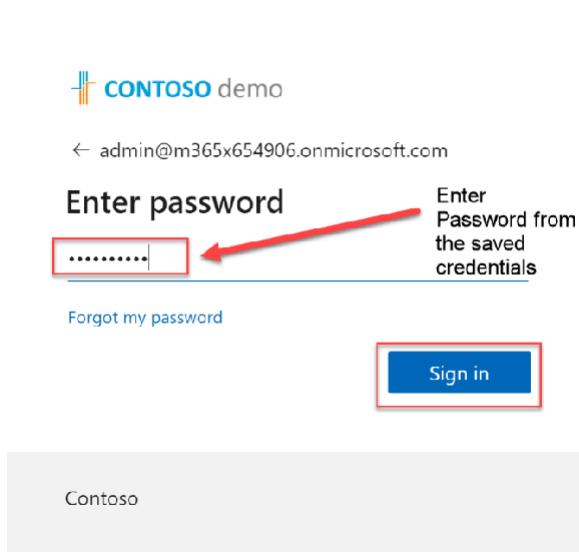
**You can use Compliance Score as a tool to track all of your risk assessments. It provides workflow capabilities to help you efficiently complete your risk assessments through a common tool.**

**If you currently use [Compliance Manager](#), you'll notice that Compliance Score is now a standalone feature with a simpler, more user-friendly design to help you manage compliance more easily.**

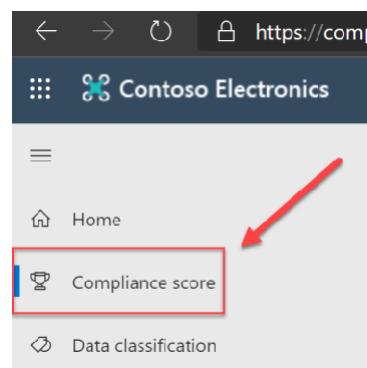
- a) Open an In-private browser (Edge)  or New in-Cognito (Chrome)
- On your machine and then go to <https://compliance.microsoft.com/homepage>
- b) Enter the admin account username that you saved in “Getting started with Microsoft 365 Compliance Master Class Labs” to gain credentials.
- c) Enter your admin credentials in the sign in as below and click NEXT



d) Enter the password and then click "Signin"



**1. On the left hand side of the portal Select Compliance Score.**



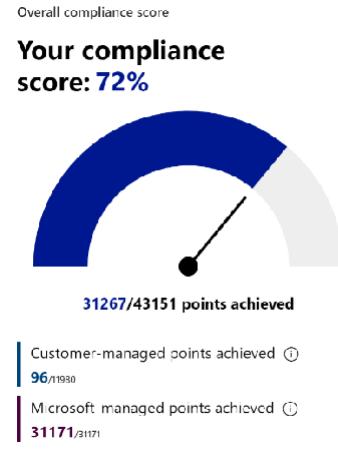
**2. You may see this message below as it sets up the Score. It should only take a few minutes to provision.**

**3. You should see the as Overview below:**

Improvement action	Impact	Test status	Group	Action type
Protect Authenticator Content	+27 points	None	Default Group	Operational
Limit Consecutive Logon Failures	+27 points	None	Default Group	Operational
Implement Account Lockout	+27 points	None	Default Group	Operational
Protect Authenticators Commensurate w...	+27 points	None	Default Group	Operational
Refresh Authenticators	+27 points	None	Default Group	Operational
Protect Wireless Access	+27 points	None	Default Group	Operational
Protect Passwords with Encryption	+27 points	None	Default Group	Operational
Manage Authenticator Lifetime and Reuse	+27 points	None	Default Group	Operational
Restrict Access to Private Keys	+27 points	None	Default Group	Operational

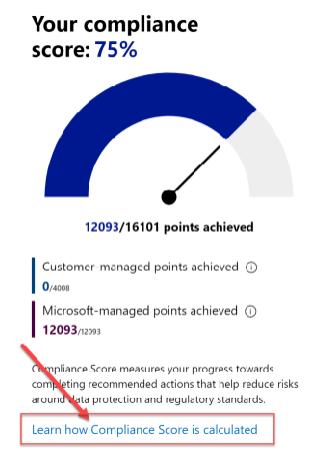
**4. Note the overall compliance score. Its important to note the following:**

- This is made up of Two parts.



- i. **Customer managed points** - these contribute to your compliance score based on controls managed by your organization
- ii. **Microsoft Managed points** - **contribute to your compliance score based on controls managed by Microsoft as a cloud service provider.**
- a. **Controls are assigned a score value based on whether they are mandatory or discretionary, and whether they are preventative, detective, or corrective—as described below.**
  - i. **Mandatory controls** are actions that cannot be bypassed either intentionally or accidentally. An example is a centrally-managed password policy that sets requirements for password length, complexity, and expiration. Users must comply with these requirements to access the system.
  - ii. **Discretionary controls** rely upon users to understand policy and act accordingly. For example, a policy requiring users to lock their computer when they leave it is a discretionary control because it relies on the user.

5. For more information on how scores are calculated please follow the link on the page as below



6. Note the Key Improvement actions. This provides a top level summary of the recommended actions. These are shown in order of highest impact which means they are the key actions to focus on first.

Improvement action	Impact	Test status	Group	Action type
Protect Authenticator Content	+27 points	● None	Default Group	Operational
Limit Consecutive Logon Failures	+27 points	● None	Default Group	Operational
Implement Account Lockout	+27 points	● None	Default Group	Operational
Protect Authenticators Commensurate wi...	+27 points	● None	Default Group	Operational
Refresh Authenticators	+27 points	● None	Default Group	Operational
Protect Wireless Access	+27 points	● None	Default Group	Operational
Protect Passwords with Encryption	+27 points	● None	Default Group	Operational
Manage Authenticator Lifetime and Reuse	+27 points	● None	Default Group	Operational
Restrict Access to Private Keys	+27 points	● None	Default Group	Operational

7. For a more detailed view - Click on Improvement actions at the top of the screen as shown below by the RED arrow. This shows all the improvement actions that you need to review and action

Improvement action	Score impact	Regulations	Group	Solutions	Assessments	Categories	Test status
Protect Authenticator Content	+27 points	Data Protection Baseline	Default Gro...	Compliance Sc...	Data Protection Baseline	Manage Compl...	● None
Limit Consecutive Logon Failures	+27 points	Data Protection Baseline	Default Gro...	Compliance Sc...	Data Protection Baseline	Manage Compl...	● None
Implement Account Lockout	+27 points	Data Protection Baseline	Default Gro...	Compliance Sc...	Data Protection Baseline	Manage Compl...	● None
Protect Authenticators Commensurate wi...	+27 points	Data Protection Baseline	Default Gro...	Compliance Sc...	Data Protection Baseline	Manage Compl...	● None
Refresh Authenticators	+27 points	Data Protection Baseline	Default Gro...	Compliance Sc...	Data Protection Baseline	Manage Compl...	● None
Protect Wireless Access	+27 points	Data Protection Baseline	Default Gro...	Compliance Sc...	Data Protection Baseline	Manage Compl...	● None
Protect Passwords with Encryption	+27 points	Data Protection Baseline	Default Gro...	Compliance Sc...	Data Protection Baseline	Manage Compl...	● None
Manage Authenticator Lifetime and Reuse	+27 points	Data Protection Baseline	Default Gro...	Compliance Sc...	Data Protection Baseline	Manage Compl...	● None
Restrict Access to Private Keys	+27 points	Data Protection Baseline	Default Gro...	Compliance Sc...	Data Protection Baseline	Manage Compl...	● None

a. Note the headings at the top of each page. These can be filtered to show just what you want to focus on. Click on Filters on top right of page. Select to show just Solutions > Information Protection and click apply.

**Microsoft Compliance Score (preview)**

Overview Improvement actions Solutions Assessments

Action you can take to improve your compliance score. Points may take up to 24 hours to update

Export 280 items Group Search Filter

Applied filters: Test Status: None +7

**Filters**

Clear filters X

Regulations

- Data Protection Baseline
- EU GDPR

Solutions

- Audit
- Azure Active Directory
- Azure Information Protection
- Cloud App Security
- Communication compliance
- Compliance Score
- Data investigation
- Data loss prevention
- Exchange
- Information governance
- Information protection
- Intune
- Microsoft 365 admin center
- Office 365 Advanced Threat Protection
- OneDrive for Business
- Power BI
- Records management
- Security & compliance center
- Service trust portal
- SharePoint Online
- Windows 10

Apply Cancel

At the top left of the page click on “Export”. This will allow you to create provide a copy of the report in CSV format. This is useful when preparing for any audits by downloading detailed reports from the assessment that combine Microsoft’s and our organization’s assessment information into a single Excel file that can be provided to internal and external auditors and regulators.

**Microsoft Compliance Score (preview)**

Overview Improvement actions Solutions Assessments

Action you can take to improve your compliance score. Points may take up to 24 hours to update.

Export

b. Return to the Improvement Actions page and clear the filters. In the search bar enter Multi

Actions you can take to improve your compliance score. Points may take up to 24 hours to update.

Export

15 items Group Mult

Filter

c. Click on Enable Multi-factor Authentication for Non-Admins

## Microsoft Compliance Score (preview)

Overview Improvement actions Solutions Assessments

Actions you can take to improve your compliance score. Points may take up to 24 hours to update.

Export

5 items

Group

Mult

Search Bar

Filter

Applied filters: Test Status: None +7 X

Improvement action	Score impact	Regulations	Group	Solutions	Assessments	Categories
Register Users for Multi-Factor Authentication	+27 points	Data Protection Baseline	Default Gro...	Azure Active Di...	Data Protection Baseline	Control Acc...
Require Mobile Devices to Wipe on Multiple Sign-in Failures	+27 points	Data Protection Baseline	Default Gro...	Intune	Data Protection Baseline	Manage Dev...
Enable Multi-factor Authentication for Admins	+27 points	Data Protection Baseline	Default Gro...	Azure Active Di...	Data Protection Baseline	Control Acc...
Enable Multi-factor Authentication for Non-Admins	+27 points	Data Protection Baseline	Default Gro...	Azure Active Di...	Data Protection Baseline	Control Acc...
Review Sign-ins After Multiple Failures Report Weekly	+1 points	Data Protection Baseline	Default Gro...	Azure Active Di...	Data Protection Baseline	Control Acc...

d. At the top shows you the status of this control. Note the Implementation Status and Implementation Date of this control

Microsoft Compliance Score > Improvement actions > Enable Multi-factor Authentication for Non-Admins

### Enable Multi-factor Authentication for Non-Admins

Points achieved

0/27

Implementation status

Not Implemented

Implementation date

Not Implemented

Test status

Not Tested

Test date

Not Tested

Assigned to

None

Group

Default Group

Edit status

e. Under “At a glance” Expand out the controls. Note the detail of each control that this applies to.

## Enable Multi-factor Authentication for Non-Admins

Points achieved <b>0/27</b>	Implementation status Not Implemented	Implementation date Not Implemented	Test status Not Tested	Test date Not Tested	Assigned to None	Group Default Group
<a href="#">Edit status</a>						
<b>At a glance</b>		<b>Implementation</b>			<b>Notes and Documentation</b>	
<p>This action is part of following standards and regulatory requirements</p> <p>Data Protection Baseline</p>		<p><b>How to implement</b></p> <p>Your organization should implement multi-factor authentication (MFA) for your users to provide an additional layer of security to protect against compromised credentials and phishing attacks. For PCI DSS Compliance, your organization should incorporate multi-factor authentication for access to the cardholder data environment. Click <b>Launch Now</b> to go to the MFA settings blade in the Azure portal. Select all users and then click <b>Enable</b>. When prompted, click <b>enable multi-factor authentication</b>.</p> <p><a href="#">Launch Now</a></p> <p><b>Learn More</b> <a href="#">How it works: Azure Multi-Factor Authentication</a> <a href="#">Deploy cloud-based Azure Multi-Factor Authentication</a> <a href="#">Configure Azure Multi-Factor Authentication settings</a></p>			<p>Uploaded documents</p> <p><a href="#">Manage documents</a></p> <p>Implementation notes</p> <p><a href="#">Edit implementation notes</a></p> <p>Test notes</p> <p><a href="#">Edit test notes</a></p> <p>Additional notes</p> <p><a href="#">Edit additional notes</a></p>	
<p><b>This action is part of following standards and regulatory requirements</b></p> <p>Data Protection Baseline</p> <p>Control ID: MSDP-IA-2(1)</p> <p>Control title: Identification and Authentication - Organizational Users - Multifactor Authentication</p> <p>Control area: Identification and Authentication</p> <p>Description:</p> <p>Implement multifactor authentication for access to privileged and non-privileged accounts.</p>						

- Implementation – note the step by step instructions and Launch Now – which can take you to the implementation of the control. This is updated by Microsoft regularly so you can be sure you always have the latest implementation steps.

### Implementation

#### How to implement

Your organization should implement multi-factor authentication (MFA) for your users to provide an additional layer of security to protect against compromised credentials and phishing attacks. Click **Launch Now** to go to the MFA settings blade in the Azure portal. Select all users and then click **Enable**. When prompted, click **enable multi-factor authentication**.

[Launch Now](#)

**Learn More** [How it works: Azure Multi-Factor Authentication](#) [Deploy cloud-based Azure Multi-Factor Authentication](#) [Configure Azure Multi-Factor Authentication settings](#)

- Click on the Edit Status of this control

## Enable Multi-factor Authentication for Non-Admins

Points achieved	Implementation status	Implementation date	Test status	Test date	Assigned to	Group
0/27	Could Not Be Detected	Not Implemented	Could Not Be Detected	03/25/2020	None	UK

Edit status



- h. Click in the assigned to box – Assign it to the MOD Administrator and Save and close
- i. Look at the Implementation Status options. Choose Implementation status – Planned. Save and close. This will email the MOD Administrator.

## Edit status for "Enable Multi-factor Authentication for Non-Admins"

Assigned to

MOD Administrator

Implementation status

Implementation date

Test status

Test date

- j. In another tab go to outlook.office.com. In your inbox should be an email similar to below showing there is an action for the user in Compliance manager. Click on View Action Item Assigned to you.

The screenshot shows the Microsoft Outlook inbox for 'MOD Administrator'. A red arrow points to the subject line of an email from 'msstmsg@microsoft.com' titled 'Compliance Manager. Action - Enable Multi-factor Authentication for Non-Admins has been assigned to you with Medium priority.' The email body contains a blue button labeled 'View Action Item Assigned to you' with a red arrow pointing to it.

- k. This opens the control. Go to the Notes and Documentation

## Enable Multi-factor Authentication for Non-Admins

Points achieved	Implementation status	Implementation date	Test status	Test date	Assigned to	Group
27/27	Alternative Implementation	5/1/2020	Passed	6/1/2020	MOD Administrator	Default Group

[Edit status](#)

At a glance		Implementation	Notes and Documentation
<b>This action is part of following standards and regulatory requirements</b>		<b>How to implement</b> Your organization should implement multi-factor authentication (MFA) for your users to provide an additional layer of security to protect against compromised credentials and phishing attacks. For PCI DSS Compliance, your organization should incorporate multi-factor authentication for access to the cardholder data environment. Click <a href="#">Launch Now</a> to go to the MFA settings blade in the Azure portal. Select all users and then click <b>Enable</b> . When prompted, click <a href="#">enable multi-factor authentication</a> .	<a href="#">Uploaded documents</a> <a href="#">Manage documents</a> <span style="border: 1px solid red; padding: 2px;">Select Manage Documents</span> <a href="#">Implementation notes</a> <a href="#">Edit implementation notes</a> <a href="#">Test notes</a> <a href="#">Edit test notes</a> <a href="#">Additional notes</a> <a href="#">Edit additional notes</a>
<a href="#">Data Protection Baseline</a>		<a href="#">Launch Now</a>  <a href="#">Learn More</a> How it works: Azure Multi-Factor Authentication Deploy cloud-based Azure Multi-Factor Authentication Configure Azure Multi-Factor Authentication settings	

Here you would attach the relevant document that was used to pass the assessment. However for the purpose of this lab we will just create a test word document. Open Microsoft Word. Create a new blank document. Enter Test passed and save. Upload the document and close.

**Manage documents for "Enable Multi-factor Authentication for Non-Admins"**

Add document

Name ↑	Added by	Date added	File size
--------	----------	------------	-----------

### I. You can now see the Test document

## Enable Multi-factor Authentication for Non-Admins

Points achieved	Implementation status	Implementation date	Test status	Test date	Assigned to	Group
27/27	Alternative Implementation	5/1/2020	Passed	6/1/2020	MOD Administrator	Default Group

[Edit status](#)

At a glance		Implementation	Notes and Documentation
<b>This action is part of following standards and regulatory requirements</b>		<b>How to implement</b> Your organization should implement multi-factor authentication (MFA) for your users to provide an additional layer of security to protect against compromised credentials and phishing attacks. For PCI DSS Compliance, your organization should incorporate multi-factor authentication for access to the cardholder data environment. Click <a href="#">Launch Now</a> to go to the MFA settings blade in the Azure portal. Select all users and then click <b>Enable</b> . When prompted, click <a href="#">enable multi-factor authentication</a> .	<a href="#">Uploaded documents</a> <span style="border: 1px solid red; padding: 2px;">Test document for Auditdock</span> <a href="#">Manage documents</a> <span style="border: 1px solid red; padding: 2px;">Select Manage Documents</span> <a href="#">Implementation notes</a> <a href="#">Edit implementation notes</a> <a href="#">Test notes</a> <a href="#">Edit test notes</a> <a href="#">Additional notes</a> <a href="#">Edit additional notes</a>
<a href="#">Data Protection Baseline</a>		<a href="#">Launch Now</a>  <a href="#">Learn More</a> How it works: Azure Multi-Factor Authentication Deploy cloud-based Azure Multi-Factor Authentication Configure Azure Multi-Factor Authentication settings	

### m. Select Edit ImplementationNotes

[Microsoft Compliance Score](#) > [Improvement actions](#) > [Enable Multi-factor Authentication for Non-Admins](#)

## Enable Multi-factor Authentication for Non-Admins

Points achieved <b>27/27</b>	Implementation status Alternative Implementation	Implementation date 5/31/2020	Test status <span style="color: green;">Passed</span>	Test date 5/31/2020	Assigned to MOD Administrator	Group Default Group
---------------------------------	---	----------------------------------	--	------------------------	----------------------------------	------------------------

[Edit status](#)

### At a glance

This action is part of following standards and regulatory requirements

[Data Protection Baseline](#)

### Implementation

#### How to implement

Your organization should implement multi-factor authentication (MFA) for your users to provide an additional layer of security to protect against compromised credentials and phishing attacks. For PCI DSS Compliance, your organization should incorporate multi-factor authentication for access to the cardholder data environment. Click [Launch Now](#) to go to the MFA settings blade in the Azure portal. Select all users and then click **Enable**. When prompted, click **enable multi-factor authentication**.

[Launch Now](#)

[Learn More](#) [How it works: Azure Multi-Factor Authentication](#)  
[Deploy cloud-based Azure Multi-Factor Authentication](#) [Configure Azure Multi-Factor Authentication settings](#)

### Notes and Documentation

#### Uploaded documents

 [Test document for Audit.docx](#)

#### Manage documents

#### Implementation notes

[Edit implementation notes](#)

#### Test notes

[Edit test notes](#)

#### Additional notes

[Edit additional notes](#)

a. Add implementation notes and click Save.

### Edit Implementation notes for "Enable Multi-factor Authentication for Non-Admins"

#### Implementation notes

All users across all locations have been registered successfully.

[Save and close](#)[Cancel](#)

b. Select Edit Test notes

Microsoft Compliance Score > Improvement actions > Enable Multi-factor Authentication for Non-Admins

## Enable Multi-factor Authentication for Non-Admins

Points achieved  
**27/27**

Implementation status  
Alternative Implementation

Implementation date  
5/31/2020

Test status  
Passed

Test date  
5/31/2020

Assigned to  
MOD Administrator

Group  
Default Group

[Edit status](#)

### At a glance

This action is part of following standards and regulatory requirements

Data Protection Baseline

### Implementation

#### How to implement

Your organization should implement multi-factor authentication (MFA) for your users to provide an additional layer of security to protect against compromised credentials and phishing attacks. For PCI DSS Compliance, your organization should incorporate multi-factor authentication for access to the cardholder data environment. Click [Launch Now](#) to go to the MFA settings blade in the Azure portal. Select all users and then click **Enable**. When prompted, click **enable multi-factor authentication**.

[Launch Now](#)

[Learn More](#) [How it works: Azure Multi-Factor Authentication](#)  
[Deploy cloud-based Azure Multi-Factor Authentication](#) [Configure Azure Multi-Factor Authentication settings](#)

### Notes and Documentation

#### Uploaded documents

[Test document for Audit.docx](#)

#### Manage documents

#### Implementation notes

[Edit implementation notes](#)

#### Test notes

[Edit test notes](#)

#### Additional notes

[Edit additional notes](#)

a. Add test notes and click Save.

## Edit Test notes for "Enable Multi-factor Authentication for Non-Admins"

### Test notes

All users have logged in successfully. [Signoff](#) by Bert Simpson (Service Delivery Manager) at 18:00

[Save and close](#)

[Cancel](#)

b. Click Edit Status

Microsoft Compliance Score > Improvement actions > Enable Multi-factor Authentication for Non-Admins

### Enable Multi-factor Authentication for Non-Admins

Points achieved 0/27	Implementation status Planned	Implementation date Not Implemented	Test status Not Assessed	Test date Not Tested	Assigned to MOD Administrator	Group Default Group
-------------------------	----------------------------------	--	-----------------------------	-------------------------	----------------------------------	------------------------

[Edit status](#)

c. Update the Implementation Status as per screen shot below.

**Edit status for "Enable Multi-factor Authentication for Non-Admins"**

Assigned to: MOD Administrator

Implementation status: Alternative Implementation

Implementation date: Mon Jun 01 2020

Test status: Passed

Test date: Mon Jun 01 2020

8. Return to the Overview page. Scroll down to see Solutions that affect your Score. Click on “View All Solutions link”.

Microsoft 365 admin center - Home Microsoft Compliance Score - Microsoft 365 compliance Mail - MOD Administrator - Outlook Microsoft Compliance Score - Microsoft 365 compliance

Contoso Electronics Microsoft 365 compliance

12120/16101 points achieved

Customer-managed points achieved 27/4008

Microsoft-managed points achieved 12093/12093

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

View all improvement actions

Solutions that affect your score

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

Solution	Score contribution	Ref
Audit	0/70 points	12
Azure Active Directory	27/416 points	25
Entire Information Protection	0/37 points	1

[View all solutions](#)

- a. This view shows all the Actions Via Solutions perspective. Scroll down to see all the solutions (grouping available)

The screenshot shows the Microsoft Compliance Score (preview) page for Contoso Electronics. The left sidebar includes links for Home, Compliance score, Data classification, Data connectors, Alerts, Reports, Policies, Permissions, Catalog, More resources, Customize navigation, and Show all. The main content area is titled "Microsoft Compliance Score (preview)" and shows a table of solutions. The table has columns for Solutions, Description, Current score contribu..., Potential score remain..., Categories, Regulations, and Action Types. Solutions listed include Audit, Azure Active Directory, Azure Information Protection, Cloud App Security, Communication compliance, Compliance Score, Data investigation, Data loss prevention, and Exchange. A red box highlights the first row, "Audit". At the bottom of the table, there is a note: "Disclaimer: Compliance Score is a dashboard that provides an overview of your organization's compliance posture across various categories. It does not provide a detailed audit or assessment of individual controls or policies." Below the table, there is a "21 items" link and a "Filter" button.

9. Switch back to the Overview page and scroll down to Compliance Score breakdown. This shows and view by Categories.

The screenshot shows the "Compliance score breakdown" page. At the top, there are tabs for Categories and Assessments, with Categories selected. Below the tabs, there are four main categories: Protect information, Govern information, Control Access, and Manage devices. Each category has a progress bar, a percentage value, and a points achieved value. Under each category, there is a brief description and a "View improvement actions" button. The categories and their details are:

- Protect information:** 0% /1541 points achieved. Description: Enable and configure encryption, control access to information, and prevent data leakage and exfiltration. Button: View improvement actions.
- Govern information:** 0% /737 points achieved. Description: Protect sensitive information and prevent its inadvertent disclosure. Button: View improvement actions.
- Control Access:** 3% /4/1931 points achieved. Description: Configure authentication and password settings, user and sign-in risk policies, and review access reports. Button: View improvement actions.
- Manage devices:** 0% /2255 points achieved. Description: Use device configuration profiles, implement malicious code and spam protection, secure mobile devices, and block unwanted applications. Button: View improvement actions.

## Part 2 - Compliance Assessments

- Click on Assessments – This shows the view of the assessments that have been created.  
Note that these are a point in time assessment and **NOT current status**.

# Compliance Manager

 Compliance Manager settings

Overview Improvement actions Solutions Assessments Assessment templates

Assessments help you implement data protection controls specified by compliance, security, privacy, and data protection standards, regulations, and laws. Assessments include actions that have been taken by Microsoft to protect your data, and they're completed when you take action to implement the controls included in the assessment. Learn how to manage assessments

 Add assessment

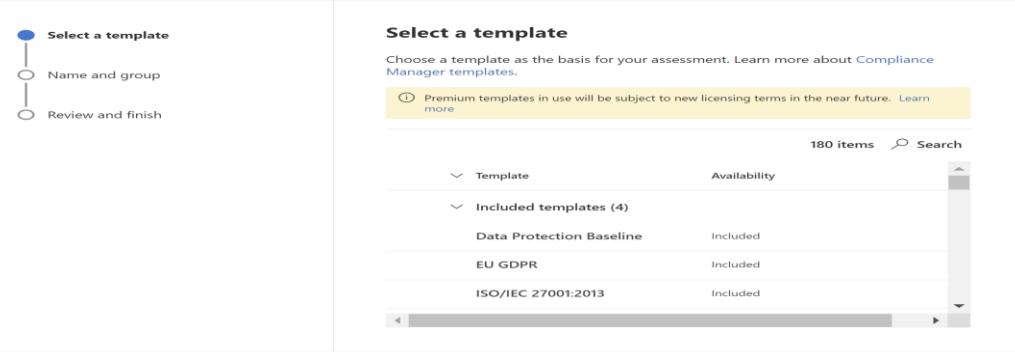
3 items  Search  Filter  Group ▾

Applied filters:

Assessment	Status	Assessment progress	Your improvement act...	Microsoft actions	Group	Product	Regulation
HIPAA	Incomplete	65%	3 of 177 completed	195 of 195 completed	Default Group	Microsoft 365	HIPAA/HITECH
New Assessment	Not started	88%	0 of 7 completed	34 of 34 completed	Default Group	Microsoft 365	Australia Spam Act
Data Protection Baseline	Incomplete	70%	6 of 499 completed	835 of 835 completed	Default Group	Microsoft 365	Data Protection Baseline

## 2. Click on Add Assessments in Compliance Manager

### Create assessment



**Select a template**

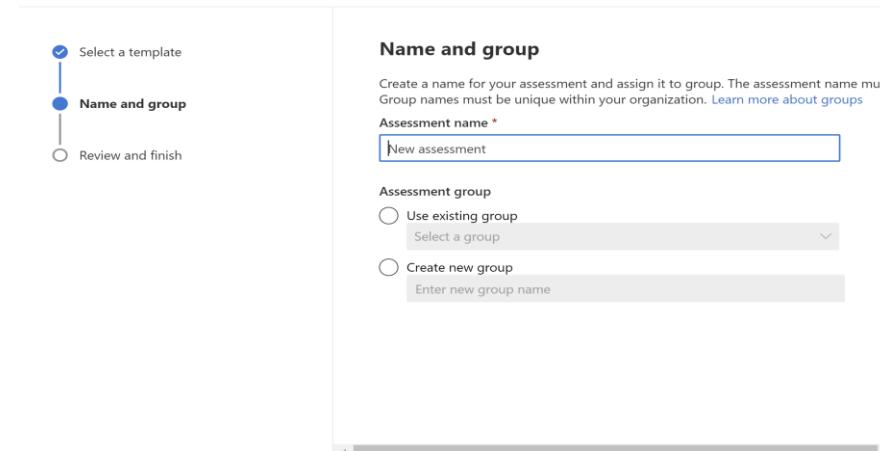
Choose a template as the basis for your assessment. Learn more about [Compliance Manager templates](#).

( ⓘ Premium templates in use will be subject to new licensing terms in the near future. Learn more )

Template	Availability
Included templates (4)	
Data Protection Baseline	Included
EU GDPR	Included
ISO/IEC 27001:2013	Included

## 3. Select a template and Click Next

### Create assessment



**Name and group**

Create a name for your assessment and assign it to group. The assessment name must be unique within the group. Group names must be unique within your organization. [Learn more about groups](#)

Assessment name \*

Assessment group

Use existing group

Create new group

Give a name to the assessment and the use the existing default Office365 group

## Create assessment

- Select a template
- Name and group
- Review and finish

### Name and group

Create a name for your assessment and assign it to group. The assessment name must be unique within the group. Group names must be unique within your organization. [Learn more about groups](#)

Assessment name \*

GDPR

Assessment group

Use existing group

Default Group

Create new group

Enter new group name

Click on Next and Create the assessment

## Create assessment

- Select a template
- Name and group
- Review and finish

### Review assessment and finish

#### Template

EU GDPR

[Edit template selection](#)

#### Name and group

GDPR

Default Group

[Edit assessment name and group](#)

d. Click on the new Assessment GDPR

## GDPR

Status      Created  
● In progress      11/2/2020

[Generate report](#)[Overview](#)   [Controls](#)   [Your improvement actions](#)   [Microsoft actions](#)

Review details about this assessment and understand your progress toward completion.

### 49% Assessment progress

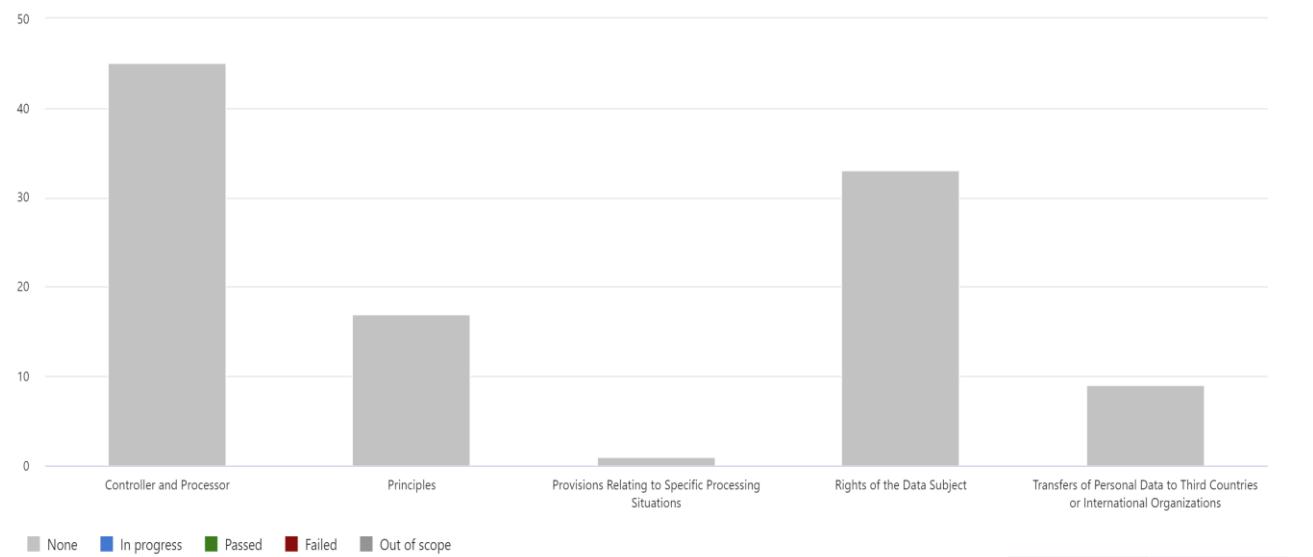
1083/2169

Your points achieved ⓘ  
0/1086

Microsoft managed points achieved ⓘ  
1083/1083

- e. Select Controls Info Tab and you can now see the In Scope Services for this assessment

Control status breakdown



- f. You can now see all the GDPR Actions that are required by the Customer. Use the dropdown arrow so see the controls under Access Control and review the details

Control title	Status	Control ID	Points achieved	Your improvement actions	Microsoft actions
 Controller and Processor (45)					
 Principles (17)					
 Provisions Relating to Specific Processing Situations (1)					
 Rights of the Data Subject (33)					
 Transfers of Personal Data to Third Countries or International Organizations (9)					

Scroll down to see the control title and details

Overview    Controls    Your improvement actions    Microsoft actions

Review improvement actions managed by your organization. Select an improvement action to edit its status and view implementation guidance.

#### Improvement action status

 None   Not assessed   Passed   Failed low risk   Failed medium risk   Failed high risk   Out of scope   To be detected   Could not be detected   Partially tested

Filter

 Filter:

Control family: Any ▾   Status: Any ▾

100 items 

Improvement action	Test status	Impact	Points achieved	Regulations	Solution	Action type	Control family
--------------------	-------------	--------	-----------------	-------------	----------	-------------	----------------

Navigate to see the Improvement actions tab

Improvement action	Test status	Impact	Points achieved	Regulations	Solution	Action type	Control family
Adhere to retention periods defined	 None	+9 points	0/9	EU GDPR	Compliance Ma...	Operational	Principles, Provisions Relating ...
Adopt security, technical, and administrative me...	 None	+9 points	0/9	EU GDPR	Compliance Ma...	Operational	Principles, Controller and Proc...
Apply Sensitivity Labels to Protect Personal Data	 None	+27 points	0/27	EU GDPR, Data Protecti...	Information pr...	Technical	Principles, Controller and Proc...
Automatically apply retention labels	 None	+27 points	0/27	EU GDPR	Records manag...	Technical	Principles, Provisions Relating ...
Complete third party information notices	 None	+9 points	0/9	EU GDPR	Compliance Ma...	Operational	Rights of the Data Subject
Confirm accuracy of collected personal data	 None	+9 points	0/9	EU GDPR, Data Protecti...	Compliance Ma...	Operational	Principles
Consumer financial incentives ont out rights	 None	+9 points	0/9	EU GDPR	Compliance Ma...	Operational	Rights of the Data Subject

Review the status of improvement actions managed by Microsoft. Select an improvement action to view details, including implementation and testing notes.

Filter

Filter

Control family: Any ▾ Status: Any ▾

55 items Search

Microsoft action	Test status	Points achieved	Regulations	Solution	Action type	Control family
1141	● Passed	9/9	EU GDPR	Compliance Ma... Contractual	Contractual	Controller and Processor
1730	● Passed	27/27	EU GDPR	Compliance Ma... Technical	Technical	Principles
AC-0100	● Passed	27/27	HIPAA/HITECH, EU GDPR, Da...	Compliance Ma... Technical	Technical	Rights of the Data Subject
AP-0100	● Passed	27/27	EU GDPR	Compliance Ma... Privacy	Privacy	Controller and Processor
AP-0200	● Passed	27/27	EU GDPR, Data Protection Ba...	Compliance Ma... Privacy	Privacy	Principles, Rights of the Data S...
AR-0100	● Passed	27/27	EU GDPR	Compliance Ma... Privacy	Privacy	Controller and Processor
AR-0102	● Passed	27/27	EU GDPR, Data Protection Ba...	Compliance Ma... Privacy	Privacy	Controller and Processor

Need help?

Give feedback

- i. You can now see the details of the control that Microsoft have implemented

Compliance Manager > Assessments > **GDPR**

## GDPR

Status In progress      Created 11/2/2020

**Generate report**

- j. You can also generate a report for the GDPR using generate report

## Adhere to retention periods defined

Points achieved	Implementation status	Implementation date	Test status	Test date	Assigned to	Group
0/9	<input checked="" type="radio"/> Not Implemented	Not Implemented	<input checked="" type="radio"/> None	None	None	Default Group

[Edit status](#)

### At a glance

This action is part of following standards and regulatory requirements

EU GDPR

EU GDPR

### Implementation

#### How to implement

Microsoft recommends that your organization determine how long data should be retained, taking into consideration the identified purposes of processing. It is recommended that your organization consider creating and maintaining Data Handling policies and standard operating procedures that document your organization's retention period(s) for personal data. We also recommend that your organization implement a process for data governance to help your organization keep data when it is needed and properly dispose of it when it is no

### Notes and documentation

Uploaded documents

[Manage documents](#)

Implementation notes

[Edit implementation notes](#)

Test notes

You can Navigate to each control ,read more information and also upload any documents related to the implementation

You have completed Part 2.

## Part 3 - Make your own Compliance template

1. Click on Assessments templates in Compliance Manager

Use a template to help you create assessments for your organization. Templates contain the controls and action data needed to track compliance with regulations, standards, and policies. [Learn about working with templates](#)

① Premium templates in use will be subject to new licensing terms in the near future. [Learn more](#)

Filter

Filters

Product scope: [Any](#) Certification: [Any](#) Created by: [Any](#)

+ Create new template Export all actions

180 items Search Group

Assessment template	Availability	Product scope	Certification	Created by	Last updated	Created
<span style="color: #f0c987;">▼ Included templates (4)</span>						
EU GDPR	: Included	Microsoft 365	EU GDPR	Microsoft	9/19/2020	9/19/2020
ISO/IEC 27001:2013	- Included	Microsoft 365	ISO 27001	Microsoft	9/19/2020	9/19/2020

Click on create new template

- Choose template type
- Upload file
- Review and finish

## Choose template type

Choose one of the options below to start creating your template. Create a custom template with your own controls and action building a custom assessment. Or, extend an existing Microsoft template with modifications to suit your needs. [Learn more about custom templates](#)

### Create a custom template

[Download the sample file](#) to see a formatted example. Fill out your template data using [these instructions](#). You'll upload your file on the next screen.

### Extend a Microsoft template

Add controls, improvement actions, or dimensions to an existing Microsoft template. Extending a template ensures you'll receive updated guidance by Microsoft as regulations change. [View the existing Microsoft templates](#)

Select Microsoft template

b. Choose a create custom template

### ● Create a custom template

[Download the sample file](#) to see a formatted example. Fill out your template data using [these instructions](#). You'll upload your file on the next screen.

c. Download the Sample template

A	B	C	D
<b>title</b>	<b>product</b>	<b>certification</b>	<b>inScopeServices</b>
Example Template	Office 365	HIPAA	Access Online;;Azure Active Directory;;Exchange Online

d. Save the file locally and you can edit if you want to change the contents and save the file

- Choose template type
- Upload file**
- Review and finish

## Upload file

Upload your formatted Excel file containing all the necessary data for your template. [View sample file](#)

Upload your template file

[Browse](#)

f. You can upload the new file with changes and finish to create the template

Choose template type

**Upload file**

Review and finish

## Upload file

Upload your formatted Excel file containing all the necessary data for your template. [View sample file](#)

Upload your template file

Browse

Upload the file, click in review and finish

Choose template type

**Upload file**

Review and finish

## Upload file

Upload your formatted Excel file containing all the necessary data for your template. [View sample file](#)

Uploaded file: Sample Template Import File - Compliance Manager.xlsx (1).xlsx

[Upload a different file](#)

## Review and finish

Review these settings to complete your template. Go back to make changes, upload a different file, or click save and finish.

Max template score

**13**

### Improvement action changes

3 new improvement actions

### Control changes

3 controls added

### Control family changes

2 control families added

# Compliance Manager

 Compliance Manager settings

Overview Improvement actions Solutions Assessments Assessment templates

Use a template to help you create assessments for your organization. Templates contain the controls and action data needed to track compliance with regulations, standards, and policies. [Learn about working with templates](#)

 Premium templates in use will be subject to new licensing terms in the near future. [Learn more](#)

Filter

 Filters

Product scope: Any ▾ Certification: Any ▾ Created by: Any ▾

+ Create new template ↗ Export all actions

181 items  Search  Group ▾

Assessment template	Availability	Product scope	Certification	Created by	Last updated	Created
<b>Included templates (5)</b>						
EU GDPR	: Included	Microsoft 365	EU GDPR	Microsoft	9/19/2020	9/19/2020

## Navigate to Compliance Manager settings

### Compliance Manager

Automated testing

Manage user history

#### Automated testing

You can set up automated testing for your Compliance Manager improvement actions that are also monitored by Secure Score. Choose to turn on automated testing for all such actions, turn off for all actions, or turn on for individual actions. [Learn more about Secure Score updates](#)

- Turn on for all improvement actions
- Turn off for all improvement actions
- Turn on per improvement action

Automated testing

Manage user history

#### Manage user history

Use these settings to manage the data of users who work with improvement actions. You can export a report of user data, delete user data, and reassign improvement actions to different users. [Learn more about these settings](#)

57 items  Search

Name

AATPSERVICE@REDACTED.onmicrosoft.com

 Select ▾

Adams@M365xREDACTED.onmicrosoft.com

 Select ▾

AdeleV@M365xREDACTED.onmicrosoft.com

 Select ▾

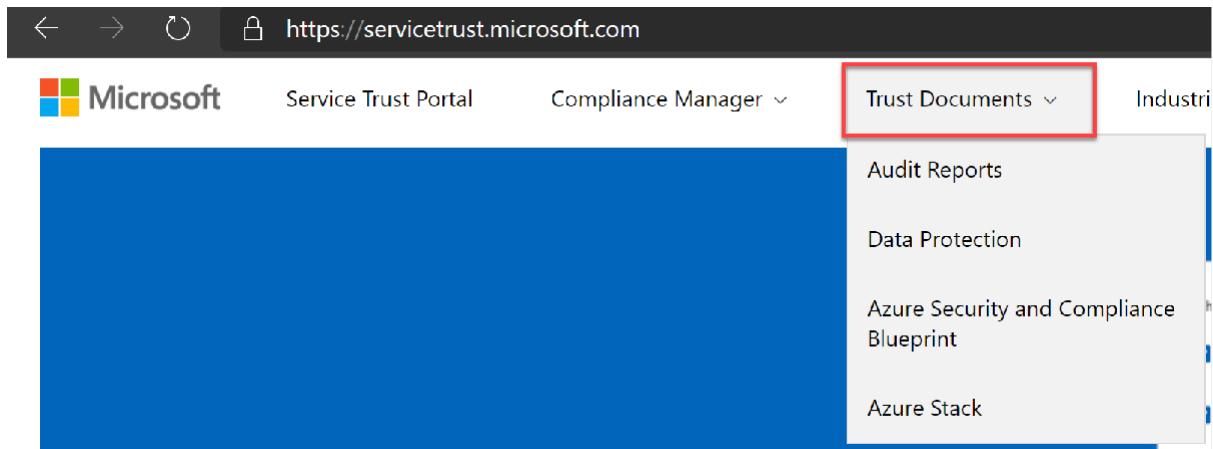
admin\_M365x0REDACTED4.onmicrosoft.com#EXT#@M365xREDACTED.onmicrosoft.com

 Select ▾

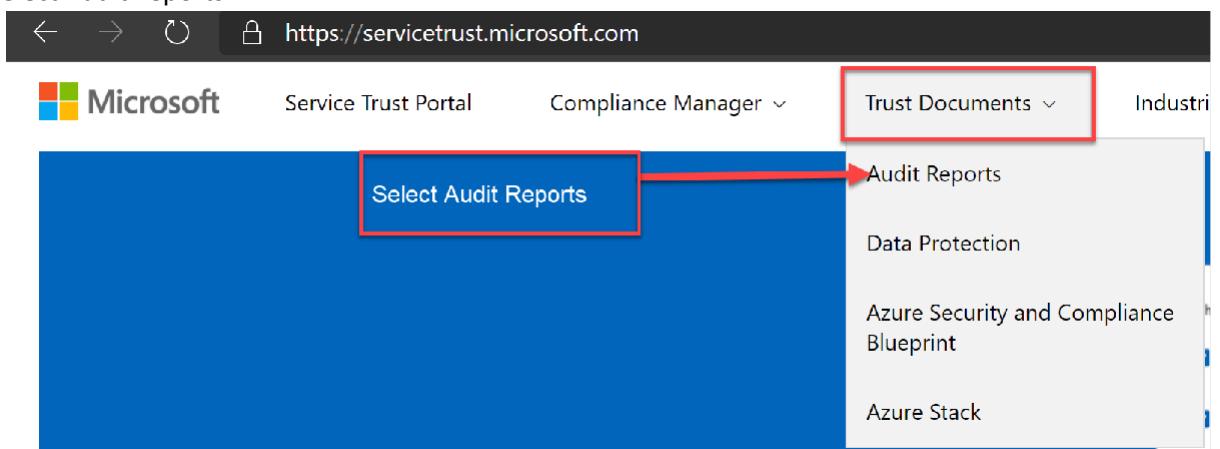
You can choose how you want to have the automated testing and then manage the user history

## Part 4 - Overview of Trust Documents

1. Browse to Service Trust Portal <https://servicetrust.microsoft.com/>
2. In here you will find Links to the Audit reports that you saw in the controls above that you created for the GDPR assessments. Click on Trust Documents



3. Select Audit Reports



4. Scroll down the page till you can see the New and Archived Audit reports.

## New and Archived Audit Reports

Use these reports to stay current on the latest privacy, security, and compliance-related information for Microsoft's cloud services.

The screenshot shows a search interface with fields for 'Select start date' and 'to' 'Select end date'. Below are dropdown menus for 'Document Type', 'Cloud Service', and 'Industries'. A horizontal navigation bar includes links for 'Azure Commercial FedRAMP', 'ENS Audit Reports and Certificates', 'FAQ and White Papers', 'FedRAMP Reports', 'GRC Assessment Reports', 'ISO Reports', and 'PCI DSS'. A red box with the text 'Use the arrow to the right to see all the report types' has an arrow pointing to a right-pointing arrow icon at the end of the bar. The main content area displays a table with columns 'Title', 'Series', 'Description', and 'Date ↓'. One row is visible: 'NERC Archival Copy - Azure Commercial FedRAMP SSP v3.05' with a download link and a date of '2019-07-26'.

5. Select SOC Reports and choose one to view. Note these documents can be downloaded for your reference or for RFP submissions etc.

## New and Archived Audit Reports

Use these reports to stay current on the latest privacy, security, and compliance-related information for Microsoft's cloud services.

The screenshot shows a search interface with fields for 'Select start date' and 'to' 'Select end date'. Below are dropdown menus for 'Document Type', 'Cloud Service', and 'Industries'. A horizontal navigation bar includes links for 'ENS Audit Reports and Certificates', 'FAQ and White Papers', 'FedRAMP Reports', 'GRC Assessment Reports', 'ISO Reports', 'PCI DSS', and 'SOC Reports'. A red box with the text 'Click the three dots to bring up the download page for a report' has an arrow pointing to a three-dot menu icon next to a report entry. The main content area displays a table with columns 'Title', 'Series', 'Description', and 'Date ↓'. Two rows are visible: 'Office 365 Microservices T2 - SSAE 18 SOC 2 Type 2 Report 9-30-2019' (with a 'NEW' badge) and 'Azure + Dynamics 365 (Public & Government) SOC 2'. To the right of each row are 'Download' and 'Save to Library' buttons. The 'SOC Reports' link in the navigation bar is also highlighted with a red box.

## Extensions

This section is not required for the Compliance Masterclass however its is an extension that you may wish to complete in your own time.

### Extension 1 - Secure Score Planner Integration

Although Secure Score is not part of this training it is integral to Compliance as well as Security.

For an overview of the new Secure Score please read <https://docs.microsoft.com/en-us/microsoft-365/security/mtp/microsoft-secure-score-new?view=o365-worldwide>

1. Browse to <https://security.microsoft.com/securescorepreview?viewid=overview>
2. On the Overview page select the first improvement action

The screenshot shows the Microsoft Secure Score Overview page. The left sidebar includes Home, Reports, Secure score (selected), Classification, Policies, Permissions, More resources, and Customize navigation. The main area displays the Microsoft Secure Score (9%), breakdown points by category (Identity 8%, Data 0%, Device 0%, Apps 20%, Infrastructure 0%), and actions to review. A red arrow points to the first improvement action: "Require MFA for administrative roles".

Improvement action	Score impact	Status	Category
Require MFA for administrative roles	+7.81%	To address	Identity
Ensure all users can complete multi-factor authentication for s...	+7.03%	To address	Identity
Enable policy to block legacy authentication	+5.47%	To address	Identity
Turn on sign-in risk policy	+5.47%	To address	Identity
Turn on user risk policy	+5.47%	To address	Identity
Stop clear text credentials exposure	+3.91%	To address	Identity
Stop legacy protocols communication	+3.91%	To address	Identity
Stop weak cipher usage	+3.91%	To address	Identity

3. To create a task in Microsoft Planner just select the **Microsoft Planner** option from the **Share** menu,

Contoso Electronics Microsoft 365 security

Improvement actions > **Require MFA for administrative roles**

Requiring multi-factor authentication (MFA) for all administrative roles makes it harder for attackers to access accounts. Administrative roles have higher permissions than typical users. If any of those accounts are compromised, critical devices and data is open to attack.

**Points achieved** 0/10 **History** No events Last synced 6/4/2020

**Manage** **Share** **Save and close** **Cancel**

1. Click Share  
2. Select Microsoft Planner

**Action plan** Microsoft teams  
Update status for Microsoft Planner Note: some statuses are system generated and can't be updated

Completed  
 To address  
 Planned  
 Risk accepted  
 Resolved through third party  
 Resolved through alternate mitigation

**Notes:**  
Write a note

**Tags:** Add tags

**At a glance**  
Category: Identity  
Protects against: [Password Cracking](#), [Account Breach](#), [Elevation of Privilege](#)  
Product: Azure Active Directory

**User impact**  
First, users with administrative roles need to register for MFA. After each admin is registered, your policies then determine when they're prompted for the additional authentication factors.

**Users affected**  
All of your Microsoft 365 global administrators  
MA [Profile] [Profile] [Profile] +2  
Show all users

**Implementation**  
**Prerequisites**  
✓ You have Azure Active Directory Premium P2.  
**Next steps**  
Standard implementation If your organization doesn't have complex security requirements, you can enable security defaults to block legacy authentication, and require registration and enablement of MFA for all users. [Learn more about how to turn on security defaults](#). Custom implementation Set up Azure Multi-factor Authentication policies to protect devices and data that are accessible by your users with administrative roles. In the on 1. Select + New Policy 2. Go to [Administratives > Users and groups > Include](#) > **Select users and groups** > check **Directory roles** 3. At a minimum, select the following roles: @ltl>@ltl> Security administrator@ltl>@ltl> Exchange service administrator@ltl>@ltl> Global administrator@ltl>@ltl> SharePoint administrator@ltl>@ltl> Helpdesk administrator@ltl>@ltl> Billing administrator@ltl>@ltl> User administrator@ltl>@ltl> Authentication administrator@ltl>@ltl> 4. Go to Cloud apps or actions > Cloud apps > Include > select **All cloud apps** (and don't exclude any apps) 5. Under Access controls > Grant > select **Grant access** > **check Require multi-factor authentication** (and nothing else) 6. Enable policy > On 7. Create Note: Classic Conditional Access policies

8. Update any fields as necessary (see suggestions below), and then select the **Create Planner Task** button to create it.

## Share to Microsoft Planner

Make sure that the people you're sharing with have permission to view it.

### Group

Operations

### Plan

IT

### Bucket

Medium priority

### Assign To (Optional)

AW Alex Wilber X

### Task name

Require MFA for administrative roles

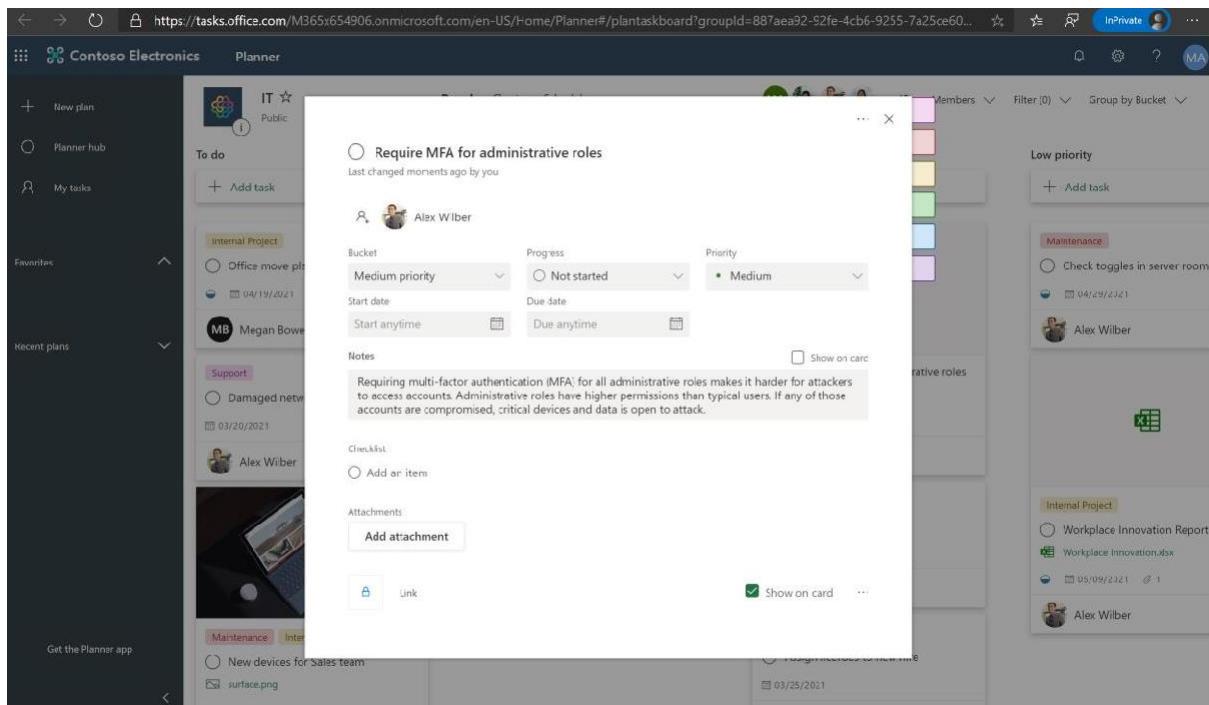
### Task description (Optional)

Requiring multi-factor authentication (MFA) for all administrative roles makes it harder for attackers to access accounts. Administrative roles have higher permissions than typical users. If any of those accounts are compromised, critical devices and data is open to attack.

Create Planner Task

Cancel

9. You may review the task in planner



## Extension 2 - Integrate ServiceNow with Microsoft Secure Score

This requires an account in ServiceNow which is a 3<sup>rd</sup> party to Microsoft. **Without a ServiceNow account you CANNOT complete this lab.**

Please follow this article to complete this part of the lab.

<https://techcommunity.microsoft.com/t5/security-privacy-and-compliance/announcing-servicenow-microsoft-teams-and-planner-integration/ba-p/914367>