



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

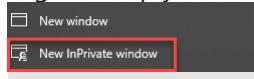
Before you start you should have completed the “Getting started with Microsoft 365 Compliance Master Class Labs”. If you have not completed this you will not be able to do this lab. You can find this document which you can download from <https://aka.ms/m365masterclass-Intro>. Each tenant will take 24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

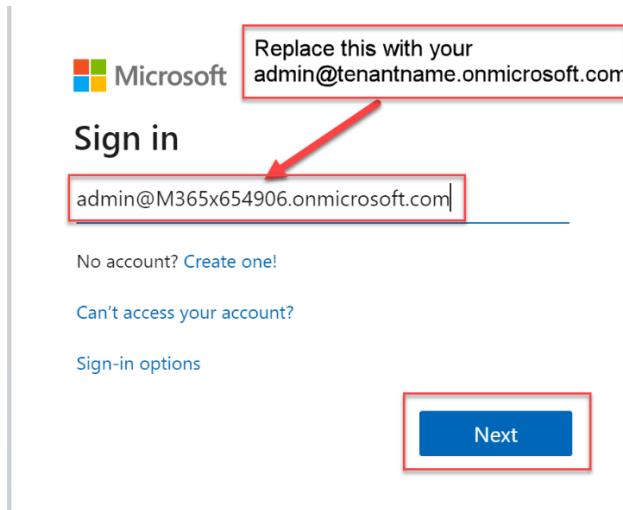
- a) Open an In-private browser (Edge)  or New in-Cognito (Chrome)



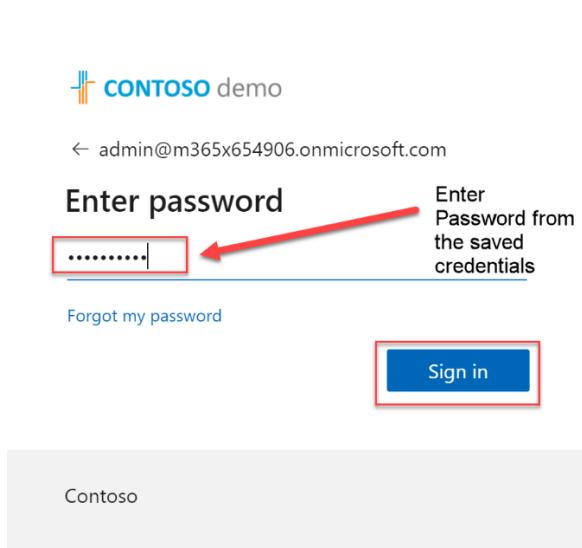
on your machine and then go to

<https://compliance.microsoft.com/homepage>

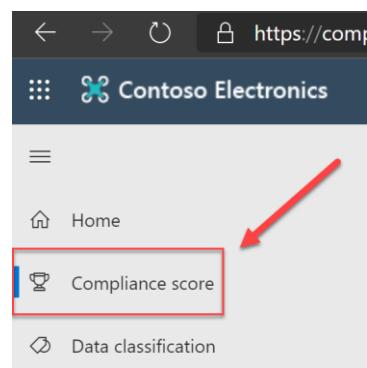
- b) Enter the admin account username that you saved in “Getting started with Microsoft 365 Compliance Master Class Labs” to gain credentials.
c) Enter your admin credentials in the sign in as below and click NEXT



- d) Enter the password and then click “Sign in”



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.

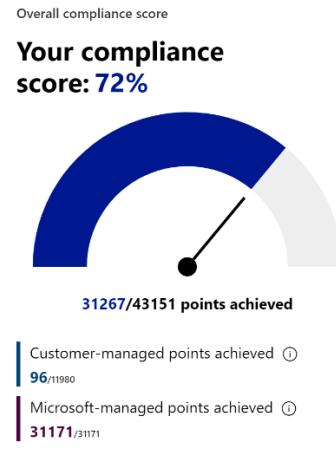
The screenshot shows the Microsoft Compliance Score (preview) interface. On the left, there's a navigation sidebar with options like Home, Compliance score, Data classification, Data connectors, Alerts, Reports, Policies, Permissions, Solutions, and Catalog. The main area is titled "Microsoft Compliance Score (preview)" and contains a message box stating "Performing first time setup..." with a note "This may take a few minutes".

3. You should see the as Overview below:

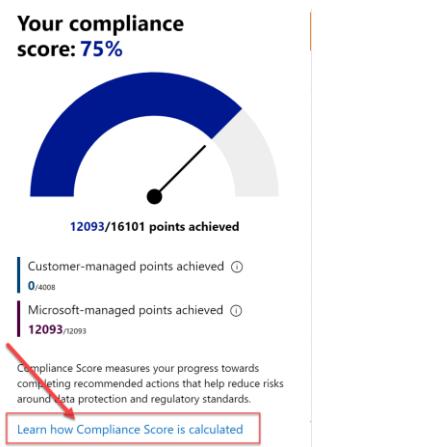
The screenshot shows the Microsoft Compliance Score (preview) Overview page. The left sidebar includes Home, Compliance score (which is selected), Data classification, Data connectors, Alerts, Reports, Policies, Permissions, Solutions, Catalog, More resources, Customize navigation, and Show all. The main content area is titled "Microsoft Compliance Score (preview)". It features a gauge chart with the text "Your compliance score: 75%" and "12093/16101 points achieved". Below the gauge, it shows "Customer-managed points achieved" (0/4008) and "Microsoft-managed points achieved" (12093/12093). A red arrow points to the "Your compliance score: 75%" text. To the right, there's a section titled "Key improvement actions" with three categories: Not completed (280), Completed (0), and Not in scope (0). A table lists various improvement actions with their details. At the bottom, there are "Need help?" and "Give feedback" buttons.

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

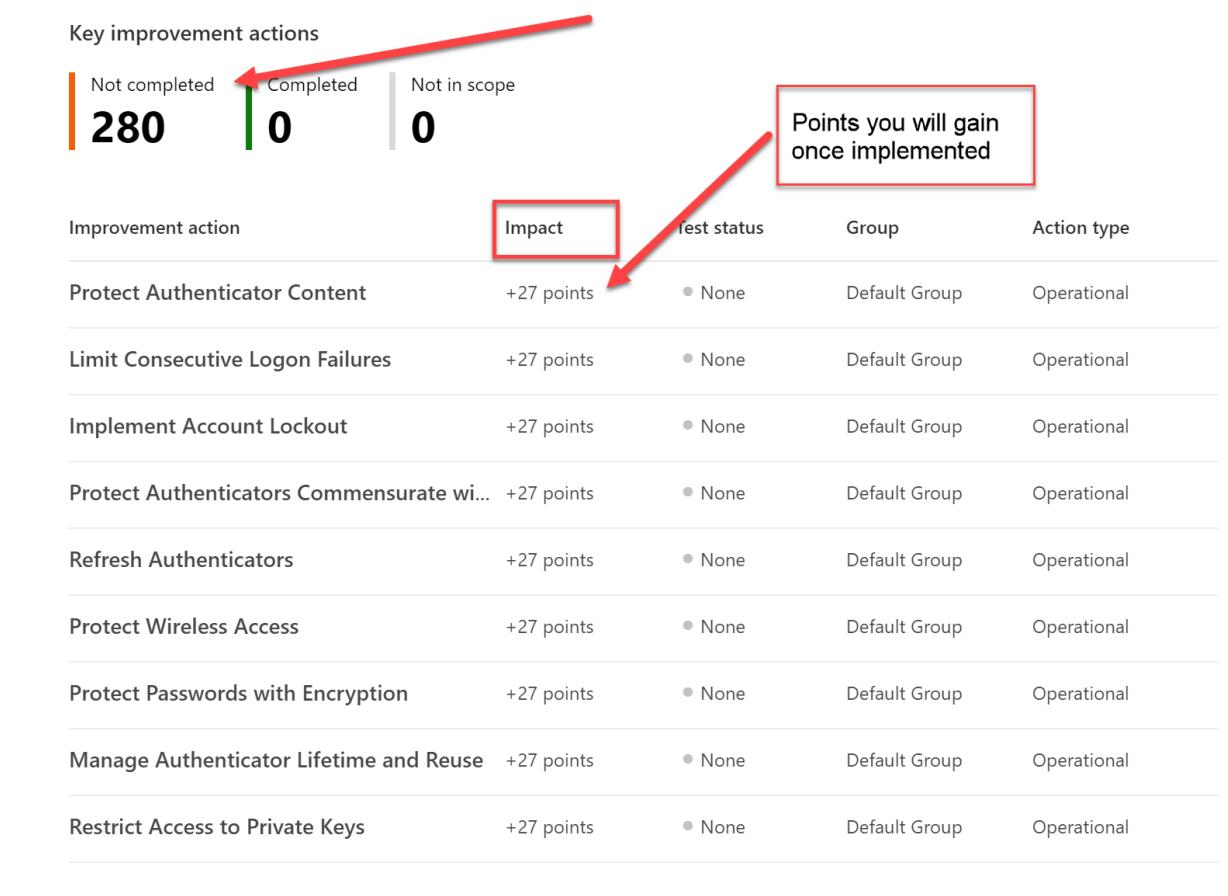
- This is made up of Two parts.



- 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.
- b. 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.



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

The figure shows the 'Improvement actions' tab selected in the navigation bar. A red arrow points to this tab. The page displays a list of 280 items, each with details like score, impact, regulations, group, solutions, assessments, categories, and test status. The table has columns for Improvement action, Score impact, Regulations, Group, Solutions, Assessments, Categories, and Test status.

| 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

Actions 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

Actions 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 Multi

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 multi

Filter

Search Bar

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 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](#)

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

[Manage documents](#)

Implementation notes

[Edit implementation notes](#)

Test notes

[Edit test notes](#)

Additional notes

[Edit additional notes](#)

This action is part of following standards and regulatory requirements

Data Protection Baseline

Control ID: MSDP-IA-2(1)

Control title: Identification and Authentication - Organizational Users - Multifactor Authentication

Control area: Identification and Authentication

Description:

Implement multifactor authentication for access to privileged and non-privileged accounts.

- 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

Planned

Implementation date

Select a date...

Test status

Not Assessed

Test date

Select a 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 365 admin center, Microsoft Compliance Score, and Microsoft Mail - MOD Administrator - Outlook tabs. The Outlook inbox contains several emails. One specific email from 'msstmsg@microsoft.com' is highlighted. The subject line is 'Compliance Manager. Action - Enable Multi-factor Authentication for Non-Admins has been assigned to you with Medium priority.' The body of the email includes a 'Compliance Score' section and a 'View Action Item Assigned to you' button. A red arrow points to this button. The email also lists other recent messages from Microsoft Azure and Contoso Electronics.

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

Enable Multi-factor Authentication for Non-Admins

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

[Edit status](#)

| | | |
|---|---|---|
| At a glance | Implementation | Notes and Documentation |
| This action is part of following standards and regulatory requirements | 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 . | Uploaded document Manage documents |
| Data Protection Baseline | Launch Now Learn More How it works: Azure Multi-Factor Authentication Deploy cloud-based Azure Multi-Factor Authentication Configure Azure Multi-Factor Authentication settings | Implementation notes Edit implementation notes |
| | | Test notes Edit test notes |
| | | Additional notes Edit additional notes |

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 27/27 | Implementation status Alternative Implementation | Implementation date 6/1/2020 | Test status Passed | Test date 6/1/2020 | Assigned to  MOD Administrator | Group Default Group |
|---------------------------------|---|---------------------------------|--|-----------------------|--|------------------------|

[Edit status](#)

| | | |
|---|---|--|
| At a glance | Implementation | Notes and Documentation |
| This action is part of following standards and regulatory requirements | 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 . | Uploaded documents  Test document for Audit.docx |
| Data Protection Baseline | Launch Now Learn More How it works: Azure Multi-Factor Authentication Deploy cloud-based Azure Multi-Factor Authentication Configure Azure Multi-Factor Authentication settings | Manage documents |
| | | Implementation notes Edit implementation notes |
| | | Test notes Edit test notes |
| | | Additional notes Edit additional notes |

m. Select Edit Implementation 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](#)

- 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](#)

- 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

Select Alternative Implementation

Enter Todays Date

Change Status to Passed

Enter todays date

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 - M | Mail - MOD Administrator - Out | Microsoft Compliance Score - M | InPrivate

Contoso Electronics Microsoft 365 compliance

12120/16101 points achieved

Customer-managed points achieved 27/4008

Microsoft-managed points achieved 12093/2093

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 | Rer |
|------------------------------|--------------------|-----|
| Audit | 0/70 points | 12 |
| Azure Active Directory | 27/416 points | 25 |
| Azure Information Protection | 0/27 points | 1 |

[View all solutions](#)

- 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 Home, Compliance score, Data classification, Data connectors, Alerts, Reports, Policies, Permissions, and a Solutions section with Catalog. The main content area is titled "Microsoft Compliance Score (preview)" and shows an overview of solutions contributing to the score. The "Solutions" tab is selected. A table lists 21 items, with the first few rows shown:

| Solutions | Description | Current score contribu... | Potential score remain... | Categories | Regulations | Action Types |
|-----------------------------|--|---------------------------|---------------------------|-----------------------|--------------------------|-------------------------|
| Audit | Search the unified audit log to view user a... | 0/70 points | 70/70 points | Discover And Respond | Data Protection Baseline | Operational,Technical |
| Azure Active Directory | Manage end user identities and access pri... | 27/416 points | 389/416 points | Control Access | Data Protection Baseline | Operational,Technical |
| Azure Information Protec... | Classify and protect documents and email... | 0/27 points | 27/27 points | Protect information | Data Protection Baseline | Technical |
| Cloud App Security | Leverage rich visibility, Control over data t... | 0/54 points | 54/54 points | Discover And Respond | Data Protection Baseline | Technical,Operational |
| Communication complia... | Monitor inappropriate communication | 0/56 points | 56/56 points | Manage Internal Risks | Data Protection Baseline | Technical,Operational |
| Compliance Score | Monitor non-compliant controls, easily as... | 0/1524 points | 1524/1524 points | Manage Compliance | Data Protection Baseline | Operational,Document... |
| Data investigation | Search for sensitive, malicious, or misplac... | 0/41 points | 41/41 points | Discover And Respond | Data Protection Baseline | Operational,Document... |
| Data loss prevention | Identify, monitor, and automatically prote... | 0/82 points | 82/82 points | Protect information | Data Protection Baseline | Technical,Operational |
| Exchange | Protect and control your organization's in... | 0/128 points | 128/128 points | Protect information | Data Protection Baseline | Operational,Technical |

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

Compliance score breakdown

The screenshot shows the "Compliance score breakdown" page. It displays four main categories: Protect information, Govern information, Control Access, and Manage devices. Each category shows a percentage achieved and a link to view improvement actions.

| Categories | Achievement (%) | Description | Action |
|-------------------------|-----------------------------------|---|--|
| Protect information | 0% 0/1543 points achieved | Enable and configure encryption, control access to information, and prevent data leakage and exfiltration | View improvement actions |
| Govern information | 0% 0/237 points achieved | Protect sensitive information and prevent its inadvertent disclosure | View improvement actions |
| Control Access | 3% 54/1593 points achieved | Configure authentication and password settings, user and sign-in risk policies, and review access reports | View improvement actions |
| Manage devices | 0% 0/2295 points achieved | Use device configuration profiles, implement malicious code and spam protection, secure mobile devices, and block unwanted applications | View improvement actions |
| Discover And Respond | 0% 0/622 points achieved | Configure audit and alert policies, discover non-compliant applications, review and correlate audit records, and review alerts, activity, access, and detection reports | View improvement actions |
| Protect Against Threats | 0% 0/1089 points achieved | Prevent, detect, investigate, and respond to advanced threats. Protect assets from unauthorized users, and devices application | 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**.

Microsoft 365 compliance

Microsoft Compliance Score (preview)

Overview Improvement actions Solutions Assessments

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 in Compliance Manager](#)

Manage assessments in Compliance Manager Microsoft actions in Compliance Manager 1 item Search Filter Group

Applied filters:

| Assessment | Status | Assessment progress | Customer managed ac... | Microsoft managed ac... | Group | Product | Regulation |
|--------------------------|-------------|---------------------|------------------------|-------------------------|---------------|---------------|-------------|
| Data Protection Baseline | In Progress | 75% | 1 of 280 completed | 709 of 709 completed | Default Group | Microsoft 365 | Data Protec |

2. Click on Manage Assessments in Compliance Manager

Microsoft 365 compliance

Microsoft Compliance Score (preview)

Overview Improvement actions Solutions Assessments

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 in Compliance Manager](#)

Manage assessments in Compliance Manager Microsoft actions in Compliance Manager 1 item Search Filter Group

Applied filters:

| Assessment | Status | Assessment progress | Customer managed ac... | Microsoft managed ac... | Group | Product | Regulation |
|--------------------------|-------------|---------------------|------------------------|-------------------------|---------------|---------------|-------------|
| Data Protection Baseline | In Progress | 75% | 1 of 280 completed | 709 of 709 completed | Default Group | Microsoft 365 | Data Protec |

3. Assessments have not yet been migrated from the old Compliance Manager portal. This will redirect you to the older Compliance Manager portal

- a. This will bring up the sevictrustportal (old interface). Click Sign in

https://sevictrust.microsoft.com/ComplianceManager/V3

Microsoft Service Trust Portal Compliance Manager Trust Documents Industries & Regions

You have selected a free, but protected, resource

Already a Microsoft cloud services customer? Sign in to your account.

To access this resource, you must be signed in to your cloud service (Office 365, Dynamics 365, Azure, or other). Click "Sign in" to open your cloud service's sign in page. You will only need to sign in once per session.

SIGN IN >

- b. In the new portal – Click the + to add an assessment.

We are pleased to announce several new preview features available now in Microsoft Compliance Score and Microsoft Compliance Manager, including the ability to import your own assessments and review periodic updates to regulatory guidance. Please [Visit our documentation](#) to learn more.

Microsoft Compliance Score is a new standalone feature in the [Microsoft 365 compliance center](#) that provides a simplified experience for managing compliance. [Learn how it works](#) and [how to set permissions](#).

Assessments

Group: Default Group

Use this group to share tenants Compliance Score

Data Protection Baseline

Product: Microsoft 365 | Certification: Data protect...

Created: 6/1/2020 | Modified: 6/1/2020

Assessment Score: 75%

Customer Managed Actions: 1 of 280

Microsoft Managed Actions: 709 of 709

Compliance Score: 75% | Customer Managed Actions: 1/280

- c. Add the Title “GDPR Assessment”, select the EU GDPR (Office 365) template. Leave the rest as default and click SAVE

Assessment

Title: Enter Name

Please select a template: EU GDPR (Office 365)

Please select a group or add a new group

Select an existing group: Default Group

Add a new group: Enter new group

Would you like to copy the data from an existing group? Off

Please select a group name:

Implementation Details

Test Plan & Additional Information

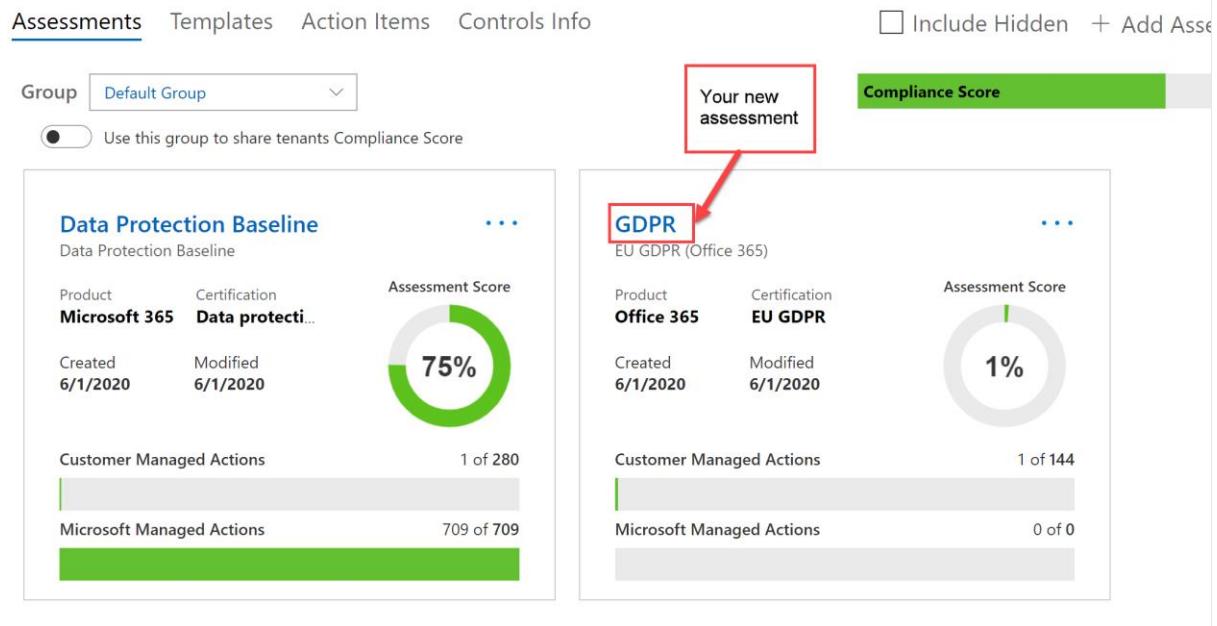
Click Save

- d. Click on the new Assessment GDPR

Assessments

We are pleased to announce several new preview features available now in Microsoft Compliance Score and Microsoft Compliance Manager, including the ability to regulatory guidance. Please [Visit our documentation](#) to learn more.

Microsoft Compliance Score is a new standalone feature in the [Microsoft 365 compliance center](#) that provides a simplified experience for managing compliance. Learn more



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

The screenshot shows the "Controls Info" tab selected in the navigation bar. It displays the following information:

- Assessed Actions:** 14/144
- Compliance Score:** 45%
- GDPR In Scope Services:**
 - Access Control: 25/25 Microsoft Assessed Actions, 3/56 Your Assessed Actions
 - Asset Management: 8/8 Microsoft Assessed Actions, 0/5 Your Assessed Actions
 - Communications Security: 4/4 Microsoft Assessed Actions, 0/24 Your Assessed Actions
 - Compliance: 3/3 Microsoft Assessed Actions, 0/2 Your Assessed Actions
 - Conditions for Collection and Processing: 8/8 Microsoft Assessed Actions, 0/4 Your Assessed Actions
 - Context of the Organization: 2/2 Microsoft Assessed Actions, 0/0 Your Assessed Actions
 - Cryptography: 2/2 Microsoft Assessed Actions, 0/10 Your Assessed Actions

- 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

Assessment Template

| Group | Default Group | Assessment | GDPR (EU GDPR (Office 365)) | Product Office 365 | Certification EU GDPR | Status Non Compliant | Modified 7 days ago | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|----------------------------------|----------------------------|-----------------------------|--------------------|-----------------------|----------------------|---------------------|--|----------|----------------------------|-----------------------|----------------|----------------------------------|----------------------------|------------------|--------------------------------|---------------------------|-------------------------|--------------------------------|----------------------------|------------|--------------------------------|---------------------------|--|--------------------------------|---------------------------|-----------------------------|--------------------------------|---------------------------|--------------|--------------------------------|----------------------------|
| Assessed Actions | 14/144 | Compliance Score | 45% | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| GDPR In Scope Services | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <table border="1"> <thead> <tr> <th>Category</th> <th>Microsoft Assessed Actions</th> <th>Your Assessed Actions</th> </tr> </thead> <tbody> <tr><td>Access Control</td><td>25/25 Microsoft Assessed Actions</td><td>3/56 Your Assessed Actions</td></tr> <tr><td>Asset Management</td><td>8/8 Microsoft Assessed Actions</td><td>0/5 Your Assessed Actions</td></tr> <tr><td>Communications Security</td><td>4/4 Microsoft Assessed Actions</td><td>0/24 Your Assessed Actions</td></tr> <tr><td>Compliance</td><td>3/3 Microsoft Assessed Actions</td><td>0/2 Your Assessed Actions</td></tr> <tr><td>Conditions for Collection and Processing</td><td>8/8 Microsoft Assessed Actions</td><td>0/4 Your Assessed Actions</td></tr> <tr><td>Context of the Organization</td><td>2/2 Microsoft Assessed Actions</td><td>0/0 Your Assessed Actions</td></tr> <tr><td>Cryptography</td><td>2/2 Microsoft Assessed Actions</td><td>0/10 Your Assessed Actions</td></tr> </tbody> </table> | | | | | | | | | Category | Microsoft Assessed Actions | Your Assessed Actions | Access Control | 25/25 Microsoft Assessed Actions | 3/56 Your Assessed Actions | Asset Management | 8/8 Microsoft Assessed Actions | 0/5 Your Assessed Actions | Communications Security | 4/4 Microsoft Assessed Actions | 0/24 Your Assessed Actions | Compliance | 3/3 Microsoft Assessed Actions | 0/2 Your Assessed Actions | Conditions for Collection and Processing | 8/8 Microsoft Assessed Actions | 0/4 Your Assessed Actions | Context of the Organization | 2/2 Microsoft Assessed Actions | 0/0 Your Assessed Actions | Cryptography | 2/2 Microsoft Assessed Actions | 0/10 Your Assessed Actions |
| Category | Microsoft Assessed Actions | Your Assessed Actions | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Access Control | 25/25 Microsoft Assessed Actions | 3/56 Your Assessed Actions | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Asset Management | 8/8 Microsoft Assessed Actions | 0/5 Your Assessed Actions | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Communications Security | 4/4 Microsoft Assessed Actions | 0/24 Your Assessed Actions | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Compliance | 3/3 Microsoft Assessed Actions | 0/2 Your Assessed Actions | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Conditions for Collection and Processing | 8/8 Microsoft Assessed Actions | 0/4 Your Assessed Actions | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Context of the Organization | 2/2 Microsoft Assessed Actions | 0/0 Your Assessed Actions | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Cryptography | 2/2 Microsoft Assessed Actions | 0/10 Your Assessed Actions | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

g. See the Total number of actions for customers and Microsoft below

Assessment Template

| Group | Default Group | Assessment | GDPR (EU GDPR (Office 365)) | Product Office 365 | Certification EU GDPR | Status Non Compliant | Modified 7 days ago | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---------------|----------------------------------|-----------------------------|--------------------|-----------------------|----------------------|---------------------|--|----------------|--|--------------|------------------|---|--|----|---------------------------|--------------|--|----------------------------------|----------------------------|-------------------|--|--|--|--|--|--|-----|---------------------------|--------------|--|-------------------|--|--|--|
| Assessed Actions | 14/144 | Compliance Score | 45% | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| GDPR In Scope Services | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <table border="1"> <thead> <tr> <th colspan="2">Access Control</th> <th>Action Score</th> <th>Related Controls</th> </tr> </thead> <tbody> <tr> <td colspan="2"> Control ID: 6.6.1.1 Control Title: Information security awareness, education and training Description Article(5)(1)(f): Personal data shall be: (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality') </td> <td>63</td> <td>No related controls found</td> </tr> <tr> <td colspan="2">Your Actions</td> <td>25/25 Microsoft Assessed Actions</td> <td>3/56 Your Assessed Actions</td> </tr> <tr> <td colspan="2">Microsoft Actions</td> <td colspan="3"></td> </tr> <tr> <td colspan="2"> Control ID: 6.6.2.1 Control Title: User registration and de-registration Description Article(5)(1)(f): Personal data shall be: (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality') </td> <td>392</td> <td>No related controls found</td> </tr> <tr> <td colspan="2">Your Actions</td> <td>Microsoft Actions</td> <td colspan="3"></td> </tr> </tbody> </table> | | | | | | | | | Access Control | | Action Score | Related Controls | Control ID: 6.6.1.1 Control Title: Information security awareness, education and training Description Article(5)(1)(f): Personal data shall be: (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality') | | 63 | No related controls found | Your Actions | | 25/25 Microsoft Assessed Actions | 3/56 Your Assessed Actions | Microsoft Actions | | | | | Control ID: 6.6.2.1 Control Title: User registration and de-registration Description Article(5)(1)(f): Personal data shall be: (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality') | | 392 | No related controls found | Your Actions | | Microsoft Actions | | | |
| Access Control | | Action Score | Related Controls | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Control ID: 6.6.1.1 Control Title: Information security awareness, education and training Description Article(5)(1)(f): Personal data shall be: (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality') | | 63 | No related controls found | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Your Actions | | 25/25 Microsoft Assessed Actions | 3/56 Your Assessed Actions | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Microsoft Actions | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Control ID: 6.6.2.1 Control Title: User registration and de-registration Description Article(5)(1)(f): Personal data shall be: (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality') | | 392 | No related controls found | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Your Actions | | Microsoft Actions | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

h. Pull down to show the actions that Microsoft have completed.

The screenshot shows the Microsoft Compliance Manager interface. At the top, there's a yellow banner with a URL and some legal text. Below it, the navigation bar includes 'Assessments', 'Templates', 'Action Items', and 'Controls Info' (which is highlighted with a red box). To the right are 'Export', 'Filter', and 'Clear' buttons. The main area has tabs for 'Assessment' (selected) and 'Template'. It shows a summary: 'Group: Default Group', 'Assessment: Data Protection Baseline (Data Protection...)', 'Product: Microsoft 365', 'Certification: Data protection baseline', 'Status: Non Compliant', and 'Modified: 7 days ago'. Below this is a progress bar: 'Assessed Actions: 20/280' and 'Compliance Score: 75%'. A section titled 'Data Protection Baseline In Scope Services' follows. Under 'Access Control', there's a table with columns 'Controls / Articles', 'Action Score', and 'Related Controls'. A red box highlights the 'Microsoft Actions' dropdown under 'Your Actions'. A red arrow points from this dropdown to the 'The control' section of the table below.

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

The screenshot shows the 'Access Control' table with two rows of data. The first row corresponds to 'Control ID: MSDP-AC-1(a)' and the second to 'Control ID: MSDP-AC-1(b)'. Each row has columns for 'Action Title', 'Compliance Score', 'Owner', 'Implementation Date & Status', and 'Test Date & Result'. A red box highlights the 'The control' section of the first row. Another red box highlights 'Status and Owner - Microsoft' in the second row. A third red box highlights 'Implementation Date' in the second row. A fourth red box highlights 'Result and Tested by' in the second row. Red arrows point from these boxes to specific details in the table, such as 'Implemented' under 'Status and Owner' and 'Passed' under 'Test Date & Result'.

j. If you select Implementation you can review the test plan that Microsoft conducted

The screenshot shows the Microsoft Compliance Manager interface. On the left, there's a list of controls under 'Your Actions'. The first control, AC-0100, is selected and shown in detail on the right. The control title is 'AC-0100' and its description is 'The organization develops, documents, and disseminates to Assignment: organization-defined personnel or roles an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.' Below this, there are four more controls listed.

Control ID: MSDP-AC-1(b)
Control Title: Access Control Policy and Description
 Assign an individual or group maintenance, authorization, distribution policy and procedures.

Control ID: MSDP-AC-1(c)
Control Title: Access Control Policy and Description
 Review and update the access control policy annually or when significant changes occur.

Control ID: MSDP-AC-1(d)
Control Title: Access Control Procedure
 Establish and document all the access control policy and associated procedures.

Control ID: MSDP-AC-1(e)
Control Title: Access Control Policies and Procedures

Action Title: AC-0100
Technical
Compliance Score: 27

Implementation Status: Implemented
Implementation Date: 8/31/2019
Test Result: Passed
Test Date: 8/31/2019

Implementation Notes:

Examined the Office 365 Information Security Policy dated 10/04/2018 and determined that Microsoft personnel have created a policy that addresses Purpose, Scope, Roles and Responsibilities, Management's Commitment, Coordination Activities and Compliance.

Examined the Microsoft Office 365 MultiTenant System Security Plan v7.0 dated 03/11/2019 and determined that Microsoft defines personnel or roles to whom the access control policy are to be disseminated as follows: Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, and BCM.

Interviewed a Principal Program Manager and a Program Manager on 03/18/2019 and determined that policies and procedures are provided to personnel on SharePoint. Assessors viewed the SharePoint repository that is leveraged for disseminating the policies and procedures and validated that

Assign User: [Assign] **Save** **Cancel**

k. Pull down to show the actions that need to be completed by the customer. Select Read more to see more details

The screenshot shows the Microsoft Compliance Manager interface. On the left, there's a list of controls under 'Your Actions'. The first control, 'Define Information System Account Types', is highlighted with a red box and a red arrow pointing to the 'Read More' link. The control title is 'Define Information System Account Types' and its description is 'Your organization should define the types of information system accounts that support your...'. Below this, there are three more controls listed.

Control ID: 6.6.1.1
Control Title: Information security awareness, education and training
 Description Article(5)(1)(f): Personal data shall be: (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures ('integrity and confidentiality')

Action Title: Define Information System Account Types
Compliance Score: 9
Owner: Review Customer
Implementation Date & Status: 63
Test Date & Result: No related controls found

Action Title: Distribute Access Control Policies and Procedures
Compliance Score: 9
Owner: Review Customer
Implementation Date & Status: 63
Test Date & Result: No related controls found

Action Title: Employ Least Privilege Access
Compliance Score: 9
Owner: Review Customer
Implementation Date & Status: 63
Test Date & Result: No related controls found

Action Title: Review Access Control Policies and Procedures
Compliance Score: 9
Owner: Review Customer
Implementation Date & Status: 63
Test Date & Result: No related controls found

You have completed Part 2.

Part 3 - Make your own Compliance template

- Click on Manage Assessments in Compliance Manager

Microsoft 365 compliance

Microsoft Compliance Score (preview)

Overview Improvement actions Solutions Assessments

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 in Compliance Manager](#)

[Manage assessments in Compliance Manager](#)

| Assessment | Status | Assessment progress | Customer managed ac... | Microsoft managed ac... | Group | Product | Regulation |
|--------------------------|-------------|---------------------|------------------------|-------------------------|---------------|---------------|-------------|
| Data Protection Baseline | In Progress | 75% | 1 of 280 completed | 709 of 709 completed | Default Group | Microsoft 365 | Data Protec |

2. Assessments have not yet been migrated from the old Compliance Manager portal. This will redirect you to the older Compliance Manager portal
 - a. This will bring up the sevictrustportal (old interface). Click Sign in

https://sevictrust.microsoft.com/ComplianceManager/V3

- b. Select the Templates Tab then Select "+ Add Template"

https://sevictrust.microsoft.com/ComplianceManager/V3/Templates

Compliance Manager (preview)

Templates

We are pleased to announce several new preview features available now in Microsoft Compliance Score and Microsoft Compliance Manager, including the ability to import your own assessments and review periodic updates to regulatory guidance. Please [Visit our documentation](#) to learn more.

Microsoft Compliance Score is a new standalone feature in the [Microsoft 365 compliance center](#) that provides a simplified experience for managing compliance. [Learn how it works](#) and [how to set permissions](#).

Assessments **Templates** Action Items Controls Info Include Hidden **+ Add Template** Filter Clear Sort

| FFIEC IS (Intune) | Product Intune | Certification FFIEC IS | Created 3/26/2020 | Modified 3/26/2020 | Customer Managed Actions 161 | Max Compliance Score 4382 | Status Approved | ... |
|-------------------|--------------------|------------------------|-------------------|--------------------|------------------------------|---------------------------|-----------------|-----|
| CSA CCM | Product Office 365 | Certification CSA CCM | Created 3/26/2020 | Modified 3/26/2020 | Customer Managed Actions 187 | Max Compliance Score 7223 | Status Approved | ... |

- c. Download the Sample template

Create a new template

Create extension from existing template

Select a template

Import template information

Browse files

A sample template with details can be accessed [here.](#)

- d. Save the Excel file locally

| Name | Status | Date modified | Type | Size |
|--|--------|------------------|-------------------------|-------|
| Sample Template Import File - Compliance Ma... | ✓ | 06/06/2020 18:17 | Microsoft Excel Work... | 20 KB |

- d. Open the downloaded excel file. For more information on how this template is structured click [here](#)
- e. On the first Tab “Template” and edit as shown below

contoso regulations.xlsx - Last Modified: 2m ago

Sensitivity: General

| | A | B | C | D |
|----|---------------------|------------|---------------|--|
| 1 | title | product | certification | inScopeServices |
| 2 | Contoso Regulations | Office 365 | Internal | Access Online;;Azure Active Directory;;Exchange Online |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |
| 8 | | | | |
| 9 | | | | |
| 10 | | | | |
| 11 | | | | |
| 12 | | | | |

Template ControlFamily Actions Dimensions

- f. Select the Second Tab “controlFamily” and Review the content. You may change it if you wish
- g. Select the third Tab “Actions” and Review the content. You may change it if you wish

- h. Select the Last Tab “Dimensions” replace the certification with Internal

| | A | B | C | D | E | F | G |
|----|----------------|----------------|---|---|---|---|---|
| 1 | dimensionKey | dimensionValue | | | | | |
| 2 | Product | Office 365 | | | | | |
| 3 | Certification | Internal | | | | | |
| 4 | Action Purpose | Preventative | | | | | |
| 5 | Action Purpose | Detective | | | | | |
| 6 | | | | | | | |
| 7 | | | | | | | |
| 8 | | | | | | | |
| 9 | | | | | | | |
| 10 | | | | | | | |
| 11 | | | | | | | |
| 12 | | | | | | | |

- i. Save the files as “Contoso regulations.xls”
- j. Return to the service trust portal
- k. Open the **Templates** dashboard and select + Add Template.
- l. Select the Templates Tab then Select “+ Add Template”

Compliance Manager (preview)

1. Click on Templates Tab

2. Click on + Add Template

| Assessments | Templates | Action Items | Controls Info | <input type="checkbox"/> Include Hidden | + Add Template | <input type="checkbox"/> Filter | <input type="checkbox"/> Clear | <input type="checkbox"/> Sort |
|-------------------|--------------------|------------------------|-------------------|---|---|----------------------------------|--------------------------------|-------------------------------|
| FFIEC IS (Intune) | Product Intune | Certification FFIEC IS | Created 3/26/2020 | Modified 3/26/2020 | Customer Managed Actions 161 Microsoft Managed Actions 181 | Max Compliance Score 4382 | Status Approved | ... |
| CSA CCM | Product Office 365 | Certification CSA CCM | Created 3/26/2020 | Modified 3/26/2020 | Customer Managed Actions 187 Microsoft Managed Actions 272 | Max Compliance Score 7223 | Status Approved | ... |

- l. Import your template data by selecting **Browse** to upload your Excel file containing the data

Template

Create a new template

Create extension from existing template

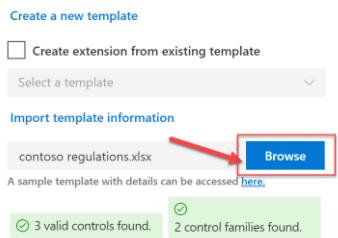
Select a template

Import template information

contoso regulations.xlsx

A sample template with details can be accessed [here](#).

3 valid controls found. 2 control families found.



2.

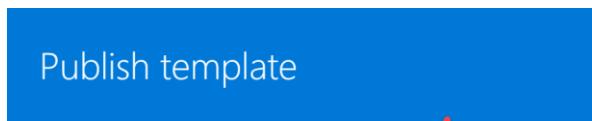
3. Select **Add to Dashboard**. You will then see your new template added to your **Templates** dashboard.

| | | | | | | | | |
|------------------------|--------------------|-------------------------|-------------------|--------------------|---|---------------------------|-----------------|-----|
| Dubai ISR (Office 365) | Product Office 365 | Certification Dubai ISR | Created 4/27/2020 | Modified 4/27/2020 | Customer Managed Actions 277 Microsoft Managed Actions 312 | Max Compliance Score 9487 | Status Approved | ... |
| Contoso Regulations | Product Office 365 | Certification Internal | Created 6/7/2020 | Modified 6/7/2020 | Customer Managed Actions 3 Microsoft Managed Actions 0 | Max Compliance Score 13 | Status Imported | ... |

4. On the hamburger Menu Right click and select Publish

| | | | | | | | | |
|-------------------------|-----------------------|-----------------------------|-------------------|--------------------|---|----------------------------|-----------------|---|
| SOC 1 (Office 365) | Product Office 365 | Certification SOC 1 | Created 3/26/2020 | Modified 3/26/2020 | Customer Managed Actions 176 Microsoft Managed Actions 94 | Max Compliance Score 3966 | Status Approved | ... |
| SOC 2 (Office 365) | Product Office 365 | Certification SOC 2 | Created 3/26/2020 | Modified 3/26/2020 | Customer Managed Actions 147 Microsoft Managed Actions 191 | Max Compliance Score 5534 | Status Approved | ... |
| LGPD (Office 365) | Product Office 365 | Certification LGPD | Created 3/26/2020 | Modified 3/26/2020 | Customer Managed Actions 358 Microsoft Managed Actions 9 | Max Compliance Score 5263 | Status Approved | ... |
| Data Protection Base... | Product Microsoft ... | Certification Data prote... | Created 3/30/2020 | Modified 3/30/2020 | Customer Managed Actions 280 Microsoft Managed Actions 709 | Max Compliance Score 16101 | Status Approved | ... |
| Dubai ISR (Office 365) | Product Office 365 | Certification Dubai ISR | Created 4/27/2020 | Modified 4/27/2020 | Customer Managed Actions 277 Microsoft Managed Actions 312 | Max Compliance Score 9487 | Status Approved | ... |
| Contoso Regulations | Product Office 365 | Certification Internal | Created 6/7/2020 | Modified 6/7/2020 | Customer Managed Actions 3 Microsoft Managed Actions 0 | Max Compliance Score 13 | Status Imported | <input type="button" value="Publish"/> <input type="button" value="..."/> <input type="button" value="Publish"/> <input type="button" value="Reject"/> <input type="button" value="Export as JSON"/> <input type="button" value="Export to Excel"/> |

5. Select Publish to continue



6. To complete the process you need a second delegated admin account to do the approval. Author of the template adds, and then publishes, a second admin will then change the status by Approving To complete this task in the lab please logon as meganb@replacewithyourtenantname.onmicrosoft.com, go to compliance manager, templates then change the status by Approving (same ellipsis in the templates section where you would select Publish).
7. Once approved the templates are now available to use.

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

A screenshot of the Service Trust Portal at https://servicetrust.microsoft.com. The top navigation bar includes the Microsoft logo, 'Service Trust Portal', 'Compliance Manager', and a 'Trust Documents' dropdown menu. A red box highlights the 'Trust Documents' button. A dropdown menu is open under 'Trust Documents', listing 'Audit Reports', 'Data Protection', 'Azure Security and Compliance Blueprint', and 'Azure Stack'.

A screenshot of the Service Trust Portal at https://servicetrust.microsoft.com. The top navigation bar includes the Microsoft logo, 'Service Trust Portal', 'Compliance Manager', and a 'Trust Documents' dropdown menu. A red box highlights the 'Trust Documents' button. A dropdown menu is open under 'Trust Documents', listing 'Audit Reports', 'Data Protection', 'Azure Security and Compliance Blueprint', and 'Azure Stack'.

3. Select Audit Reports

A screenshot of the Service Trust Portal at https://servicetrust.microsoft.com. The top navigation bar includes the Microsoft logo, 'Service Trust Portal', 'Compliance Manager', and a 'Trust Documents' dropdown menu. A red box highlights the 'Select Audit Reports' button. An arrow points from this button to the 'Audit Reports' link in the open 'Trust Documents' dropdown menu.

A screenshot of the Service Trust Portal at https://servicetrust.microsoft.com. The top navigation bar includes the Microsoft logo, 'Service Trust Portal', 'Compliance Manager', and a 'Trust Documents' dropdown menu. A red box highlights the 'Select Audit Reports' button. An arrow points from this button to the 'Audit Reports' link in the open 'Trust Documents' dropdown menu.

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 the search are filters for 'Document Type', 'Cloud Service', and 'Industries'. A 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 a red arrow pointing to the right edge of the page.

| Title | Series | Description | Date ↓ |
|---|--------|---|------------|
| NERC Archival Copy - Azure Commercial FedRAMP SSP v3.05 | | NERC Archival Copy - Azure Commercial FedRAMP SSP v3.05 | 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 the search are filters for 'Document Type', 'Cloud Service', and 'Industries'. A navigation bar includes links for 'ENS Audit Reports and Certificates', 'FAQ and White Papers', 'FedRAMP Reports', 'GRC Assessment Reports', 'ISO Reports', and 'PCI DSS'. A red box labeled 'SOC Reports' has a red arrow pointing to it. Another red box labeled 'Click the three dots to bring up the download page for a report' has a red arrow pointing to the three-dot menu icon next to the first report. The first report in the table is highlighted with a yellow background and a red border. The table columns are 'Title', 'Series', 'Description', and 'Date ↓'. The first row shows 'Office 365 Microservices T2 - SSAE 18 SOC 2 Type 2 Report 9-30-2019' with a 'NEW' badge. The second row shows 'Azure + Dynamics 365 (Public & Government) SOC 2'.

| Title | Series | Description | Date ↓ |
|--|--------|---|------------|
| Office 365 Microservices T2 - SSAE 18 SOC 2 Type 2 Report 9-30-2019 <small>NEW</small> | | Office 365 Microservices T2 - SSAE 18 SOC 2 Type 2 Report 9-30-2019 | 2020-05-20 |
| Azure + Dynamics 365 (Public & Government) SOC 2 | | This document details audit assessment performed by a third party independent | 2020-05-4 |

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, 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 a timeline chart. Below these are sections for 'Actions to review' (Regressed 0, To address 28, Planned 0, Risk accepted 0, Recently added 0, Recently updated 0) and 'Top improvement actions'. The first action listed is 'Require MFA for administrative roles', which is highlighted with a red box and a red arrow pointing to it from the text above. The table for 'Top improvement actions' has columns for Improvement action, Score impact, Status, and Category. Other actions listed include 'Ensure all users can complete multi-factor authentication for \$...', 'Enable policy to block legacy authentication', 'Turn on sign-in risk policy', 'Turn on user risk policy', 'Stop clear text credentials exposure', 'Stop legacy protocols communication', and 'Stop weak cipher usage'. At the bottom right are 'Need help?' and 'Give feedback' buttons.

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 **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

[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 Assignments > 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> Conditional Access administrator@ltl> @ltl> SharePoint administrator@ltl> @ltl> Helpdesk administrator@ltl> @ltl> Billing administrator@ltl> @ltl> User administrator@ltl> @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

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

The screenshot shows the Microsoft Planner interface. On the left, there's a navigation sidebar with options like 'New plan', 'Planner hub', and 'My tasks'. The main area displays a task card for 'Require MFA for administrative roles'. The card includes fields for 'Bucket' (Medium priority), 'Progress' (Not started), and 'Priority' (Medium). It also has sections for 'Notes' (warning about MFA for admin roles), 'Checklist' (with an 'Add an item' button), and 'Attachments' (a 'Link' button). To the right, there's a list of other tasks and projects, such as 'Check toggles in server room' and 'Workplace Innovation Report'. The overall theme is dark, with some light-colored cards.

Extension 2 – Integrate ServiceNow with Microsoft Secure Score

This requires an account in ServiceNow which is a 3rd 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>