

Part 9c – Compliance Manager – Improvement action

(Compliance Manager)

Contents

Disclaimer.....	2
Target Audience	2
Document Scope	2
Out-of-Scope	2
Overview of Document	3
Use Case	3
Definitions.....	3
Notes.....	4
Pre-requisites.....	4
“Decision Trees” to get to Improvement Actions	5
Improvement Actions – an Overview	5
Accessing Improvement Actions – Option #1	6
Accessing Improvement Actions – Option #2	7
Accessing Improvement Actions – Option #3	11
5 Improvement action Tabs	14
Overview (tab)	14
Implementation (tab).....	16
Testing (tab)	17
Standards and Regulations (tab).....	18
Documents (tab)	19
Technical Improvement action	20
Documentational Improvement action	24
Appendix and Links	28

Before we start, please note that if you want to see a table of contents for all the sections of this blog and their various Purview topics, you can locate them in the following link:

[Microsoft Purview- Paint By Numbers Series \(Part 0\) - Overview - Microsoft Tech Community](#)

Disclaimer

This document is not meant to replace any official documentation, including those found at docs.microsoft.com. Those documents are continually updated and maintained by Microsoft Corporation. If there is a discrepancy between this document and what you find in the Compliance User Interface (UI) or inside of a reference in docs.microsoft.com, you should always defer to that official documentation and contact your Microsoft Account team as needed. Links to the docs.microsoft.com data will be referenced both in the document steps as well as in the appendix.

All of the following steps should be done with test data, and where possible, testing should be performed in a test environment. Testing should never be performed against production data.

Target Audience

The Information Protection section of this blog series is aimed at Security and Compliance officers who need to properly label data, encrypt it where needed.

Document Scope

This document is meant to guide an administrator who is “net new” to Microsoft E5 Compliance through using Compliance Manager to run Improvement Actions based on what an assessment is indicating.

Out-of-Scope

This document does not cover any other aspect of Microsoft E5 Purview, including:

- Data Classification
- Information Protection
- Data Protection Loss (DLP) for Exchange, OneDrive, Devices
- Data Lifecycle Management (retention and disposal)
- Records Management (retention and disposal)
- eDiscovery
- Insider Risk Management (IRM)
- Priva
- Advanced Audit

- Microsoft Cloud App Security (MCAS)
- Information Barriers
- Communications Compliance
- Licensing

It is presumed that you have a pre-existing understanding of what Microsoft E5 Compliance does and how to navigate the User Interface (UI).

For details on licensing (i.e. which components and functions of Purview are in E3 vs E5) you will need to contact your Microsoft Security Specialist, Account Manager, or certified partner.

Overview of Document

This document 1) walk you through different ways to reach the **Improvement Actions** section of an assessment and 2) then how to apply recommended Improvement Actions.

- Decision Trees for getting to a Control's Improvement actions.
- 3 ways to access Improvement actions
- Review of the 5 tabs within any particular Improvement action.
- Technical Improvement action
- Documentational Improvement action

Use Case

An administrator wants to apply Improvement Actions to their tenant based-on an assessment that has been run previously, for example the one run in Part 9b of this blog series.

Definitions

- Actions– the things that need to be done to mark a Control as completed and
- Assessments – these 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.
- Assessment Templates – these templates track compliance with over 300 industry and government regulations around the world.
- Compliance Score - Compliance Manager awards you points for completing improvement actions taken to comply with a regulation, standard, or policy, and combines those points into an overall compliance score. Each action has a different impact on your score depending on the potential risks involved. Your compliance score can help prioritize which action to focus on to improve your overall compliance posture. You receive an initial score based on the Microsoft

365 data protection baseline. This baseline is a set of controls that includes key regulations and standards for data protection and general data governance.

- Controls – the various requirements in your tenant that must be met to meet a part of an assessment.
- Control Family – a group of Controls.
- Microsoft Actions – These are actions that Microsoft has performed inside of your tenant to help it meet a specific assessment.
- Progress – each assessment has a progress chart to help you visualize the progress you are making to meet the requirements of the assessment
- Your Improvement Actions – These are actions that you and your organization must perform to meet a specific assessment/certification/regulation.
- Overview – This allows you to view the specific control, it's status, scope, actions, needed, etc.
- Implementation – This will explain what you need to do in your tenant to meet this control. It will also give you and update on the Implimentation status and data
- Testing – here you can alook at your Control testing history.
- Standards and Regulations – This will reference which regulations and/or certifications are relevent to this Control.
- Documentation – This is where you can place your documentation around this specific Control. This is done via the **Add Evidence** button.
- Technical Improvement action – This is not an official Microsoft term, but is one that I will use in this document to differentiate an Improvement action that requires the configuration of your tenant or Azure cloud.
- Documentational Improvement action – This is not an official Microsoft term, but is one that I will use in this document to differentiate an Improvement action that requires action or documentation outside of your tenant or Azure cloud.

Notes

None

Pre-requisites

It is recommended you read the official Microsoft documentation on Compliance Manager and Parts 9a-9b of this blog series.

It is also recommended you run a **Data Protection Baseline** and the **GDPR for Microsoft Tenant** assessments. This will help you to run the Improvement actions in this blog entry.

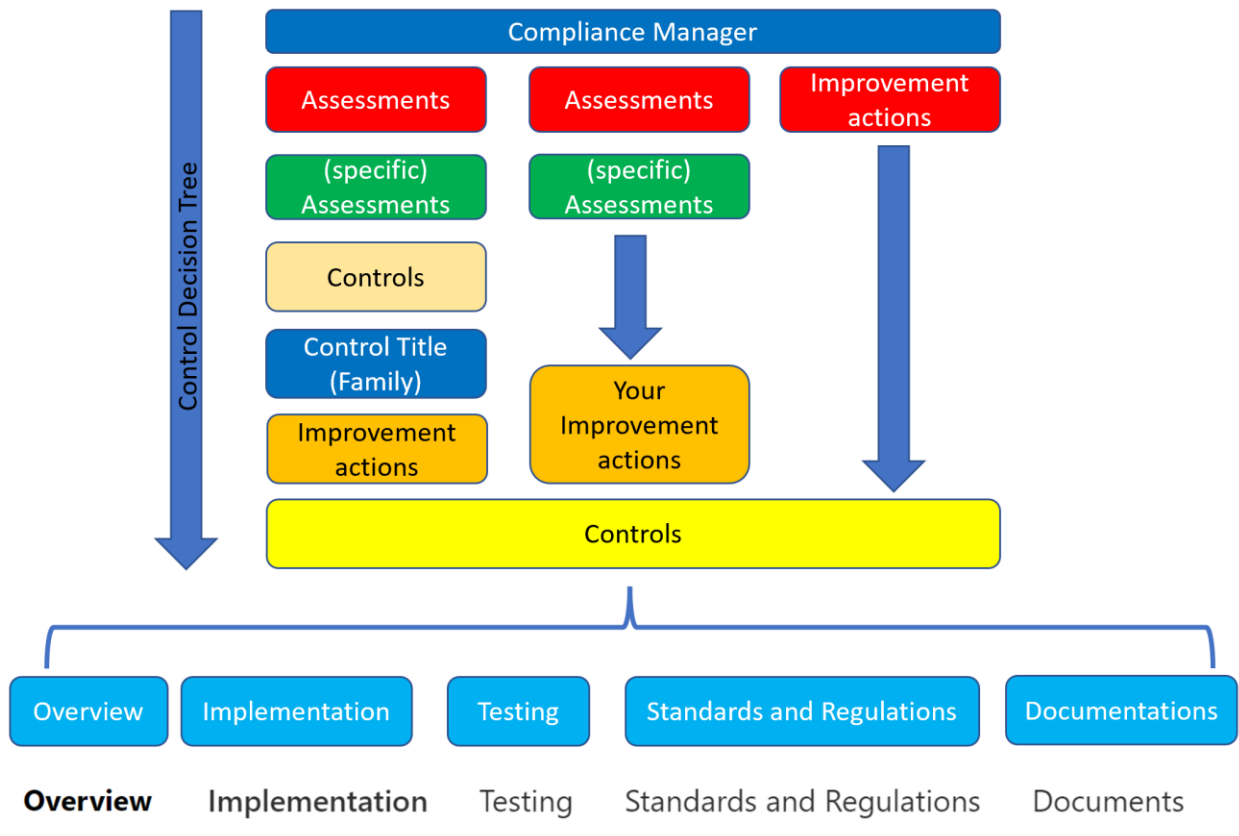
You will need administrative rights on aad.portal.azure.com.

“Decision Trees” to get to Improvement Actions

There are 3 ways that you can access Improvement actions section. Let us take a moment to look at how you can get to a Control’s Improvement action(s). Here are the 3 paths you can take:

- From within core Compliance Manager, go to the Improvement actions tab -> (Specific) Improvement Action you want to run.
- From within your assessment, go to the Control (tab) -> Controls Family -> Controls -> Implementation
- From within your assessment, go to the Your Improvement Actions (tab) -> (Specific) Improvement Actions -> Controls -> Implementation

See the diagram below for how these two “decision trees” appear visually.



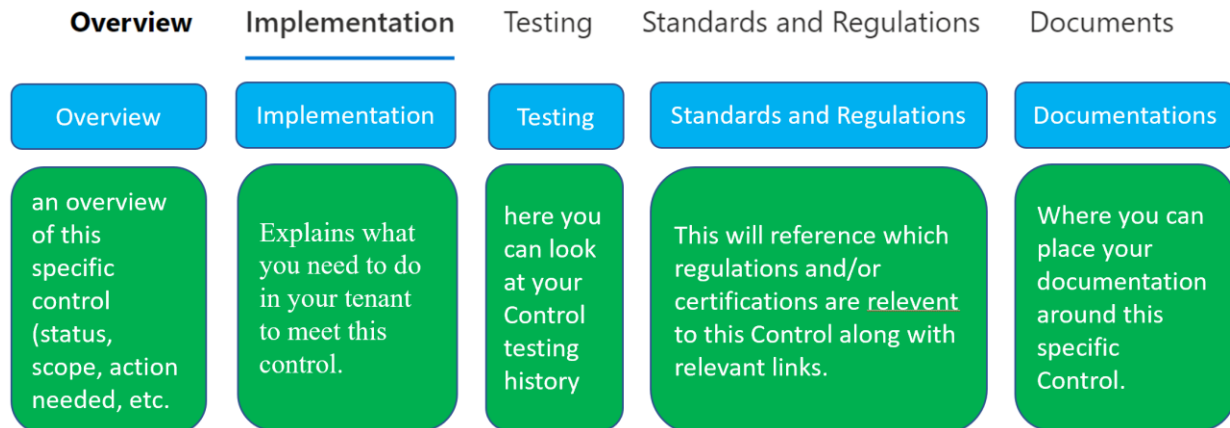
Below, we will walk through each of these “decision trees”

Improvement Actions – an Overview

Once you are in a specific Improvement action, you will see 5 tabs across the top. Here is what each of the tabs do, plus a visual diagram of those same tabs and what they do.

1. Overview – This allows you to view the specific control, it’s status, scope, actions, needed, etc.

2. Implementation – This will explain what you need to do in your tenant to meet this control. It will also give you an update on the Implementation status and data
3. Testing – here you can look at your Control testing history.
4. Standards and Regulations – This will reference which regulations and/or certifications are relevant to this Control.
5. Documentation – This is where you can place your documentation around this specific Control. This is done via the **Add Evidence** button.



Accessing Improvement Actions – Option #1

The first way to arrive at this **Improvement actions** page is as follows:

1. Go to **Compliance Manager** -> **Improvement actions**

Compliance Manager

Overview Improvement actions Solutions

2. On the bottom, you will find the list of all Improvement Actions. Click on one.

<input type="checkbox"/>	Improvement action	Products
<input type="checkbox"/>	Enable self-service password reset	Microsoft 365
<input type="checkbox"/>	Conceal informatio... Pending update	Microsoft 365
<input type="checkbox"/>	Use boundary protection devices...	Microsoft 365
<input type="checkbox"/>	Provide just-in-time notification ...	Microsoft 365

3. You will then land on the **Improvement actions** page.

[Compliance Manager](#) > Improvement actions > Enable self-service password reset

E Enable self-service password reset

i This action is automatically monitored. [Learn more](#)

Overview	Implementation	Testing	Standards and Regulations	Documents
Details	Implementation status			
Implementation Status	● Partially Implemented			
Partially Implemented	Implementation date			
Test Status	Not Available			
Points achieved				

4. We will cover what each of these tabs in the 5 “tab” sections below. After that, we will detail how to run these Improvement Actions in the sections labeled Technical Improvement Action and Documentational Improvement actions.

Accessing Improvement Actions – Option #2

The second way to arrive at this **Improvement actions** page is as follows:

1. Go to **Compliance Manager -> Assessments – (Specific) Assessment** (in this case Data Protection Baseline)

Compliance Manager




Overview Improvement actions Solutions Assessments Assessment temp

Assessments help you implement data protection controls specified by compliance, security, privacy, and other requirements. Microsoft has taken action to protect your data, and they're completed when you take action to improve your data protection.

Activated/Licensed templates

2/0

[View details](#)

 Add assessment  Add Recommended Assessments  Export actions  Update actions

Assessment	Status	Assessment progress	Your improvements
<input type="checkbox"/> GDPR for Microsoft Tenant	Incomplete	21%	3 of 118
<input type="checkbox"/> HIPAA	Pending update Incomplete	48%	6 of 389
<input type="checkbox"/> HiTrust	Pending update Incomplete	47%	7 of 682
<input type="checkbox"/> Data Protection Ba...	Pending update Incomplete	51%	11 of 821

2. On the right side, click on the **Controls** tab and at the bottom select an Improvement action

Progress Controls Your improvement actions

3. Scroll down to the **Control title** section, and select your specific Control Family and (Specific) control

>	Control title	Status
∨	Controller and Processor (45)	
	Agreements	None
	Allocation of Responsibilities for Joint Controllers	None
	Authorization for the Engagement of Other Proces...	None

4. This will take you to the page for your **Improvement actions** and **Microsoft's Improvement actions**. You do not need to worry about the Microsoft Improvement actions as they will be maintained by Microsoft inside your tenant. Below **Improvement actions**, click a your (specific) Improvement action you want to take.

Improvement actions

Microsoft actions

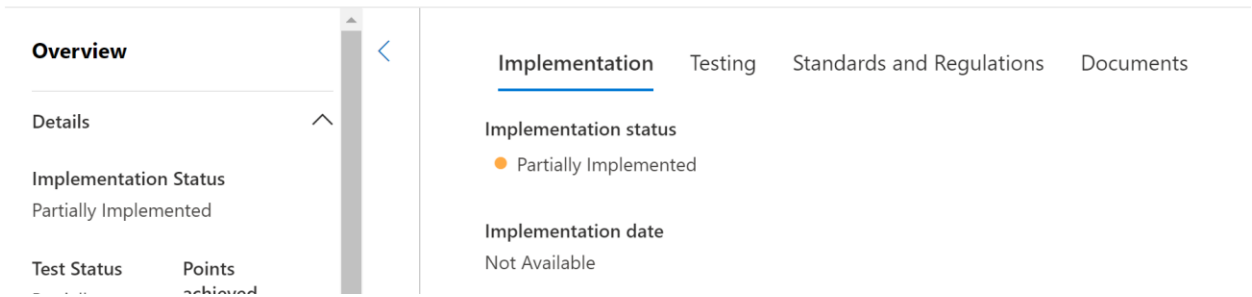
■ None ■ Not assessed ■ Passed ■ Failed low risk

Improvement action	Products
Define the duties of processors	Microsoft 365
Determine organization role in pro...	Microsoft 365
Include requirements on processin...	Microsoft 365

5. You will then land on the **Improvement actions** page.

E Enable self-service password reset

 This action is automatically monitored. [Learn more](#)



Overview

Details

Implementation Status
Partially Implemented

Test Status Points achieved

Implementation Testing Standards and Regulations Documents

Implementation status
● Partially Implemented

Implementation date
Not Available

5. We will cover what each of these tabs in the 5 “tab” sections below. After that, we will detail how to run these Improvement Actions in the sections labeled Technical Improvement Action and Documentational Improvement actions.

Accessing Improvement Actions – Option #3

The second way to arrive at this **Improvement actions** page is as follows:

1. Go to **Compliance Manager -> Assessments – (Specific) Assessment** (in this case Data Protection Baseline)

Compliance Manager

Overview Improvement actions Solutions **Assessments** Assessment temp

Assessments help you implement data protection controls specified by compliance, security, privacy, and regulatory requirements. Some of these controls have already been taken by Microsoft to protect your data, and they're completed when you take action to improve your data protection.

Activated/Licensed templates

2/0

[View details](#)

 Add assessment  Add Recommended Assessments  Export actions  Update actions

	Assessment	Status	Assessment progress	Your improvements
<input type="checkbox"/>	GDPR for Microsoft Tenant	Incomplete	21%	3 of 118
<input type="checkbox"/>	HIPAA Pending update	Incomplete	48%	6 of 389
<input type="checkbox"/>	HiTrust Pending update	Incomplete	47%	7 of 682
<input type="checkbox"/>	Data Protection Ba... Pending update	Incomplete	51%	11 of 828

2. On the right side, click on the **Your Improvements actions** tab and at the bottom select an Improvement action

Review improvement actions managed by your organization. Select an improvement implementation guidance.

Improvement action status

None Not assessed Passed Failed low risk Failed medium risk

Accept all updates

Filter  Reset  Filters

Control family: **Any** ▾


Status: **Any** ▾

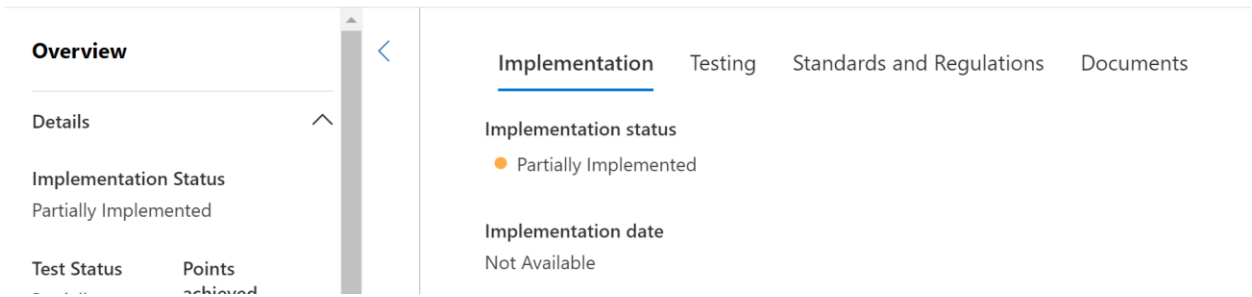
Testing Source: **Any** ▾

Improvement action	Products	Test status
Adhere to defined retention peri...	Microsoft 365	<input type="radio"/> None
Adopt security, technical, and ad...	Microsoft 365	<input type="radio"/> None
Audit user query event paramete...	Microsoft 365	<input type="radio"/> None
Automatically appl... Pending update	Microsoft 365	<input checked="" type="radio"/> Passed

3. You will then land on the **Improvement actions** page.

E Enable self-service password reset

 This action is automatically monitored. [Learn more](#)



Overview

Details

Implementation Status
Partially Implemented

Test Status Points achieved

Implementation Testing Standards and Regulations Documents

Implementation status
● Partially Implemented

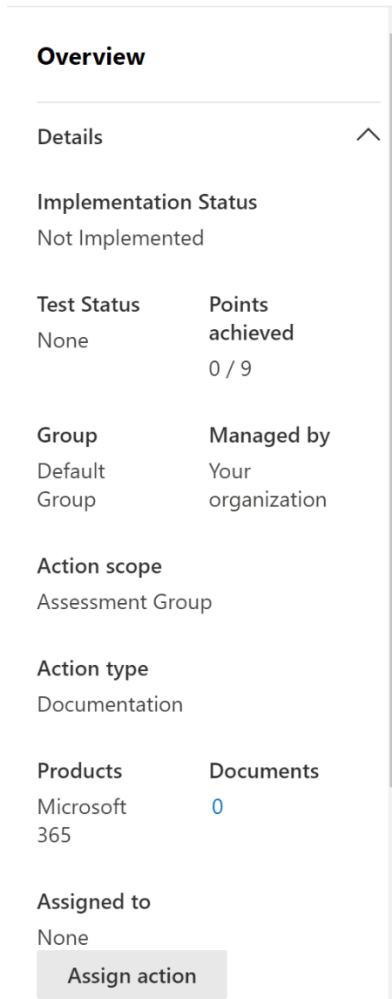
Implementation date
Not Available

4. We will cover what each of these tabs in the 5 “tab” sections below. After that, we will detail how to run these Improvement Actions in the sections labeled Technical Improvement Action and Documentational Improvement actions.

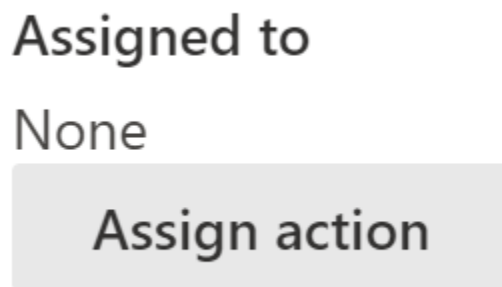
5 Improvement action Tabs

Overview (tab)

On the left-side you will find the **Overview** tab. This will show of this specific Improvement action you are trying to run, its status, scope, action needed, etc.



1. At the bottom of the **Overview** tab you will also see an item labeled **Assign action**. As you might expect, this will allow you to assign a specific user to implement this control (ex. Bob Smith or Jane Young). This will then be tracked inside the **Overview** tab.



2. **Testing Source** can be select below the **Assign action** button. For more information Testing Sources, see this link **Working with Improvement Actions** which is in the

Appendix and Links section below. Here are a few excerpts from the official documentation to help you understand at a fundamental level.

“For those improvement actions that can be automatically tested, you'll see the Automatic option for testing source. Compliance Manager will detect signals from other compliance solutions you've set up in your Microsoft 365 environment, as well as any complementary actions that Microsoft Secure Score also monitors.”

“Automatic testing is on by default for all eligible improvement actions. You can adjust these settings to automatically test only certain improvement actions, or you can turn off automatic testing for all actions.

“When you select Parent as the testing source for an improvement action, you'll choose another action to which your action will be linked. Your action in effect becomes the "child" to the action that you designate as the "parent." When you designate a parent for an improvement action, that action will inherit the implementation and testing details of the parent action. Any time the parent action's status changes, the child's status will inherit those changes. The child action will also accept all evidence in its Documents tab that belong to the parent action, which could override any data that previously existed in the child action's Documents.”

Testing Source

A rectangular dropdown menu with a thin black border. The text "Manual" is displayed on the left side, and a downward-pointing chevron icon is on the right side.

3. You can now move to the Implementation tab.

[Implementation \(tab\)](#)

On the right, you will see 4 tabs. We will start with the **Implementation** tab. This tab explains what you need to do in your tenant to meet this control.

Implementation status

- Not Available

Implementation date

Not Available

Implementation notes

[Edit implementation details](#)

How to implement

Microsoft recommends that your organization define and document the following duties of processors in written and electronic agreements:

- To process the collection, use and disclosure of the personal data only on instructions from the controller, unless such instruction is inconsistent with law or provisions relating to personal data protection
- To provide appropriate security measures to prevent loss, access, use, modification, correction, or disclosure of personal data in an unauthorized or unlawful manner
- To report data breaches
- To make and store a record of processing activities
- To assist data controller for any required action, such as responding to a data subject request
- To delete information provided by the controller once the agreement with the controller ends
- To handle and address complaints from authorized individuals or legal authorities, at the controller's direction, and notify the controller through writing or orally
- To keep proof of the authorization for the processing
- To demonstrate the privacy management programs, if requested
- To not engage other processors without written authorization from the controller
- Impose the same data protection obligations as set out in contracts or legal acts if engaging another processor for carrying out specific processing activities approved by the controller
- To remove information from information systems if knowledge is accidentally gained on facts or circumstances from an electronic record that could lead to civil or criminal liabilities
- To adhere to an approved code of conduct or certification mechanism to demonstrate compliance with organizational requirements
- To comply with relevant laws of the country in cases where the data processor is not domiciled in the country where the data is processed
- To update the information provided to the controller, according to a defined time period.

You can now move to the **Testing** tab.

[Testing \(tab\)](#)

Now let us look at the **Testing** tab. Here you can look at your Control testing history.

Implementation

Testing

Standards and Regulations

Documents

Test status

● None

Test date

Not Available

Testing notes

Additional notes

Edit testing details

Testing history

Download the history of all testing changes for this action

Export testing history

At this point there is nothing to be done on this tab, but you can revisit this tab after you have started to implement your actions and testing. Proceed to the next section.



[Standards and Regulations \(tab\)](#)

Next, we will look at the **Standards and Regulations** tab. This will reference which regulations and/or certifications are relevant to this Control. This can help you know if the Improvement action will “check off” one regulation/certification need, or multiples.

16 items

Filter  Reset  Filters

Regulation: **Any** 

> Control	Control ID	Control family	Regulation
 Data protection baseline (2)			
External Personnel Security - Contractu...	MSDP-PS-7(a)	Personnel Security	Data protection baseline
Privacy Compliance - Record Disclosure...	MSDP-PC-8	Privacy Compliance	Data protection baseline
 EU GDPR (11)			
Responsibility and Liability of the Contr...	24.1	Controller and Processor	EU GDPR
Use of Processors	28.1	Controller and Processor	EU GDPR
Authorization for the Engagement of O...	28.2	Controller and Processor	EU GDPR

Let us move to the final tab on Documentation.

Documents (tab)

Lastly, we will look at the **Documentation** tab. This is where you can place your documentation around this specific Control. This is done via the **Add Evidence** button. You can upload your spreadsheets, corporate documentation, update regulation documentation and anything else you might deem relevant for this Improvement action.

Implementation

Testing

Standards and Regulations

Documents

+ Add evidence ↓ Download all

Evidence name

Type

Let is now move to the 2 types of Improvement action. We will start with the Technical Improvement action.

Technical Improvement action

For this we will **enable self-service password reset** as our technical Control. You can take any of the “decision tree” paths mentioned above open this Improvement Action.

1. Go to **Compliance Manager** -> **Improvement actions**.

Compliance Manager

Overview

Improvement actions

2. On the right side you will find a search field. Enter “Enable self” and click search.

3 items


Group ▾

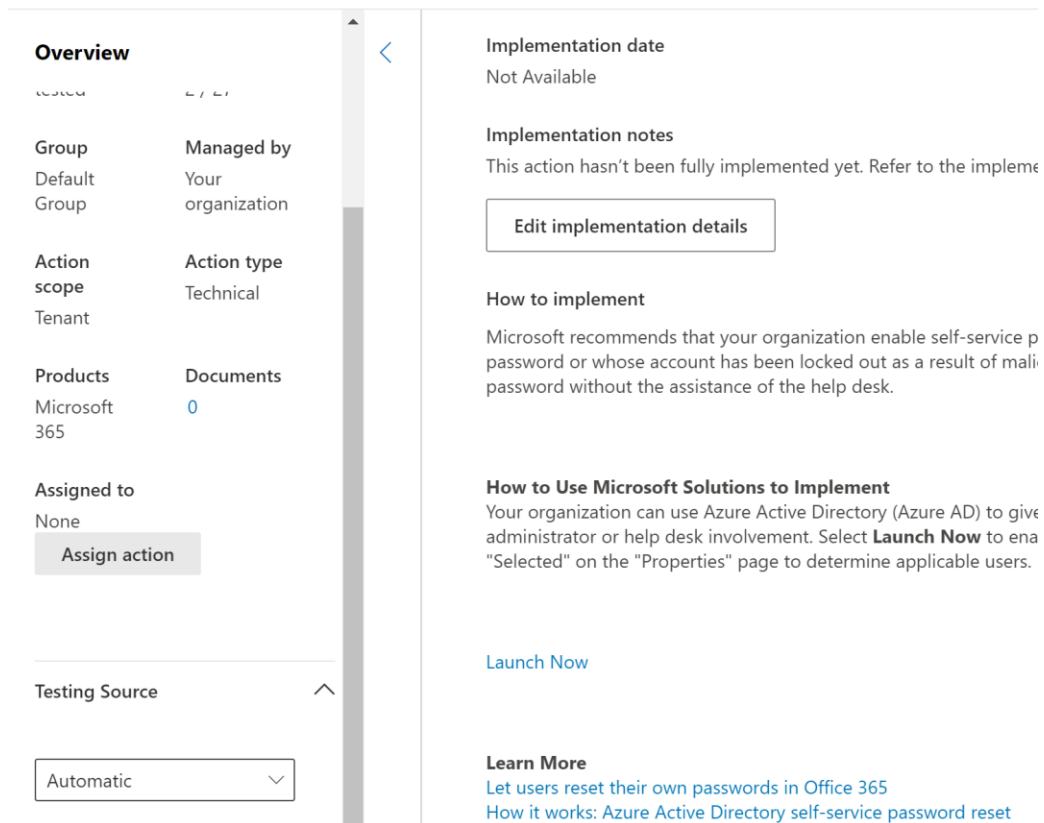
3. It will give you the following results similar to the following.

<input type="checkbox"/>	Improvement action	Products
<input type="checkbox"/>	Enable self-service password reset	Microsoft 365
<input type="checkbox"/>	Enable self-service ... Pending update	Microsoft 365
<input type="checkbox"/>	Enable self-service ... Pending update	Microsoft 365

4. Click on **enable self-service password reset**. You will then land on Implementation action.

E Enable self-service password reset

 This action is automatically monitored. [Learn more](#)



Overview

Group: Default Group
Managed by: Your organization

Action scope: Tenant
Action type: Technical

Products: Microsoft 365
Documents: 0

Assigned to: None
[Assign action](#)

Testing Source: Automatic

Implementation date
Not Available

Implementation notes
This action hasn't been fully implemented yet. Refer to the implementation guide.

[Edit implementation details](#)

How to implement
Microsoft recommends that your organization enable self-service password reset or whose account has been locked out as a result of malicious password without the assistance of the help desk.

How to Use Microsoft Solutions to Implement
Your organization can use Azure Active Directory (Azure AD) to give administrators or help desk involvement. Select **Launch Now** to enable "Selected" on the "Properties" page to determine applicable users.

[Launch Now](#)

Learn More
[Let users reset their own passwords in Office 365](#)
[How it works: Azure Active Directory self-service password reset](#)

5. Go to the Implementation tab and scroll down to **How to Use Microsoft Solutions to Implement**. Here it will tell you how to enable this Improvement action.

How to Use Microsoft Solutions to Implement

Your organization can use Azure Active Directory (Azure AD) to give users the ability to change or reset their password with no administrator or help desk involvement. Select **Launch Now** to enable Self-Service Password Reset (SSPR) by selecting "All" or "Selected" on the "Properties" page to determine applicable users.

6. After you've reviewed that documentation, scroll back up to **Launch Now** and click it.

Launch Now

7. You will be taken to the website aad.portal.azure.com.

The screenshot displays the Azure Active Directory admin center interface. The top navigation bar is blue and contains the text "Azure Active Directory admin center". Below this, the breadcrumb path is "Dashboard > Contoso > Password reset". The main heading is "Password reset | Properties" with a three-dot menu icon. Below the heading, it says "Contoso - Azure Active Directory". On the right side, there are "Save" and "Discard" buttons. The main content area shows "Self service password reset enabled" with a help icon and a selection dropdown with options "None", "Selected" (highlighted), and "All". Below this is a "Select group" section with a help icon and the group name "SSPRSecurityGroupUsers". A blue information box contains the text: "These settings only apply to end user and are required to use two authentic password policies." The left sidebar contains a navigation menu with "Dashboard", "All services", "FAVORITES", "Azure Active Directory", "Users", and "Enterprise applications". The main content area has a "Manage" section with "Diagnose and solve problems" and a "Properties" section with "Authentication methods", "Registration", "Notifications", "Customization", "On-premises integration", and "Administrator Policy". Below this is an "Activity" section with "Audit logs" and "Usage & insights". At the bottom is a "Troubleshooting + Support" section with "New support request".

8. At this point you can implement the information the steps that you read earlier.
9. Once done, this Improvement action will show as **Implemented**.

Documentational Improvement action

For this we will **adhere to defined retention periods** as our technical Control. You can take any of the “decision tree” paths mentioned above open this Improvement Action.

1. Go to **Compliance Manager -> Improvement actions**.

Compliance Manager

Overview **Improvement actions**

2. On the right side you will find a search field. Enter “adhere” and click search.

2 items

3. It will give you the following results similar to the following.

- Improvement action
- Adhere to defined retention periods
- Establish and adhere to binding corporate rules

4. Click on **adhere to defined retention periods**. You will then land on Implementation action.

Overview

Details

Implementation Status
Not Implemented

Test Status	Points achieved
None	0 / 9

Group	Managed by
Default Group	Your organization

Implementation Testing

Implementation status
● Not Available

Implementation date
Not Available

Implementation notes

[Edit implementation details](#)

5. Go to the Implementation tab and scroll down to **How to Implement**. Here it will tell you how to enable this Improvement action.

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 longer required. As a part of the retention strategy:

- Continuously review records schedules to determine if technology and/or business changes affects the records
- Determine if the retention period for any records is longer than the life of the system where they are currently stored and plan for the migration of records to a new system before the current system is retired
- Perform system upgrades of hardware and software while maintaining the functionality and integrity of the electronic records created in them.

The National Archives Universal Electronic Records Management (ERM) Requirements prescribe agencies to contact NARA of any actual, impending, or threatened unlawful removal, defacing, alteration, corruption, deletion, erasure, or other destruction of records in the custody of the agency.

Dubai Consumer Protection Regulations (Telecommunications Regulatory Authority) require licensee to retain:

- Records of post-paid Subscriber's Invoices for a period of not less than two (2) years;
- Records of Consumer Complaints for a minimum period of two (2) years;
- evidence (documentary, video, audio, etc.) as may be necessary to support advertisement compliance with these Regulations for a period of one year.

The New Zealand - Public Records Act prohibits any person to dispose of, or authorize the disposal of, public records or protected records except with the authority of the Chief Archivist, unless the disposal of a public record or a protected record is required by or under another Act.

6. Since there are no technical actions to perform in your demo tenant scroll down to **Implementation notes** and click **Edit implementation details**.

Implementation notes

[Edit implementation details](#)

7. You will then be able to enter information relevant to this Improvement action.

Edit implementation details

Implementation status

Select Implementation status...



Implementation date

Select a date...



Implementation notes

add implementation notes

8. Here you can change the Implementation status, data and notes.

Implementation status

Select Implementation status...

Not Implemented

Implemented

Alternative Implementation

Planned

Out of scope

9. Make changes to this field as desired and click **Save**.
10. You can also add documentation relevant to this Implementation action on the Documents page by clicking **Add evidence**. At this point you can implement the information the steps that you read earlier.

Implementation Testing Standards and Regulations **Documents**

[+](#) Add evidence [↓](#) Download all

Evidence name	Type
---------------	------

11. Once done, this Improvement action will show as **Implemented**.

We are now done with this basic walkthrough of the Improvement actions and how to implement them. For a better understanding of Improvement actions, please read the official documentation, some of which are listed in the Appendix and Links as well as run assessments in your test tenant.

Appendix and Links

[Microsoft Purview Compliance Manager - Microsoft Purview \(compliance\) | Microsoft Docs](#)

[Build and manage assessments in Microsoft Purview Compliance Manager - Microsoft Purview \(compliance\) | Microsoft Docs](#)

[Learn about assessment templates in Microsoft Purview Compliance Manager - Microsoft Purview \(compliance\) | Microsoft Docs](#)

[Build and manage assessments in Microsoft Purview Compliance Manager - Microsoft Purview \(compliance\) | Microsoft Docs](#)

[Working with improvement actions in Microsoft Purview Compliance Manager - Microsoft Purview \(compliance\) | Microsoft Docs](#)

[Working with improvement actions in Microsoft Purview Compliance Manager - Microsoft Purview \(compliance\) | Microsoft Docs](#)

Note: This solution is a sample and may be used with Microsoft Compliance tools for dissemination of reference information only. This solution is not intended or made available for use as a replacement for professional and individualized technical advice from Microsoft or a Microsoft certified partner when it comes to the implementation of a compliance and/or advanced eDiscovery solution and no license or right is granted by Microsoft to use this solution for such purposes. This solution is not designed or intended to be a substitute for professional technical advice from Microsoft or a Microsoft certified partner when it comes to the design or implementation of a compliance and/or advanced eDiscovery solution and should not be used as such. Customer bears the sole risk and responsibility for any use. Microsoft does not warrant that the solution or any materials provided in connection therewith will be sufficient for any business purposes or meet the business requirements of any person or organization.