#NVSummit2021

This is how you drive security and compliance process in Microsoft 365!

Ståle Hansen
Principal Cloud Architect @ CloudWay
@StaleHansen
Microsoft MVP & RD

NORDIC — VIRTUAL SUMMIT —

This is how you drive security
compliance process in

CloudWay

https://youtube.com/StaleHansen

This is how you drive security
ss in

CloudWay

https://youtube.com/StaleHansen

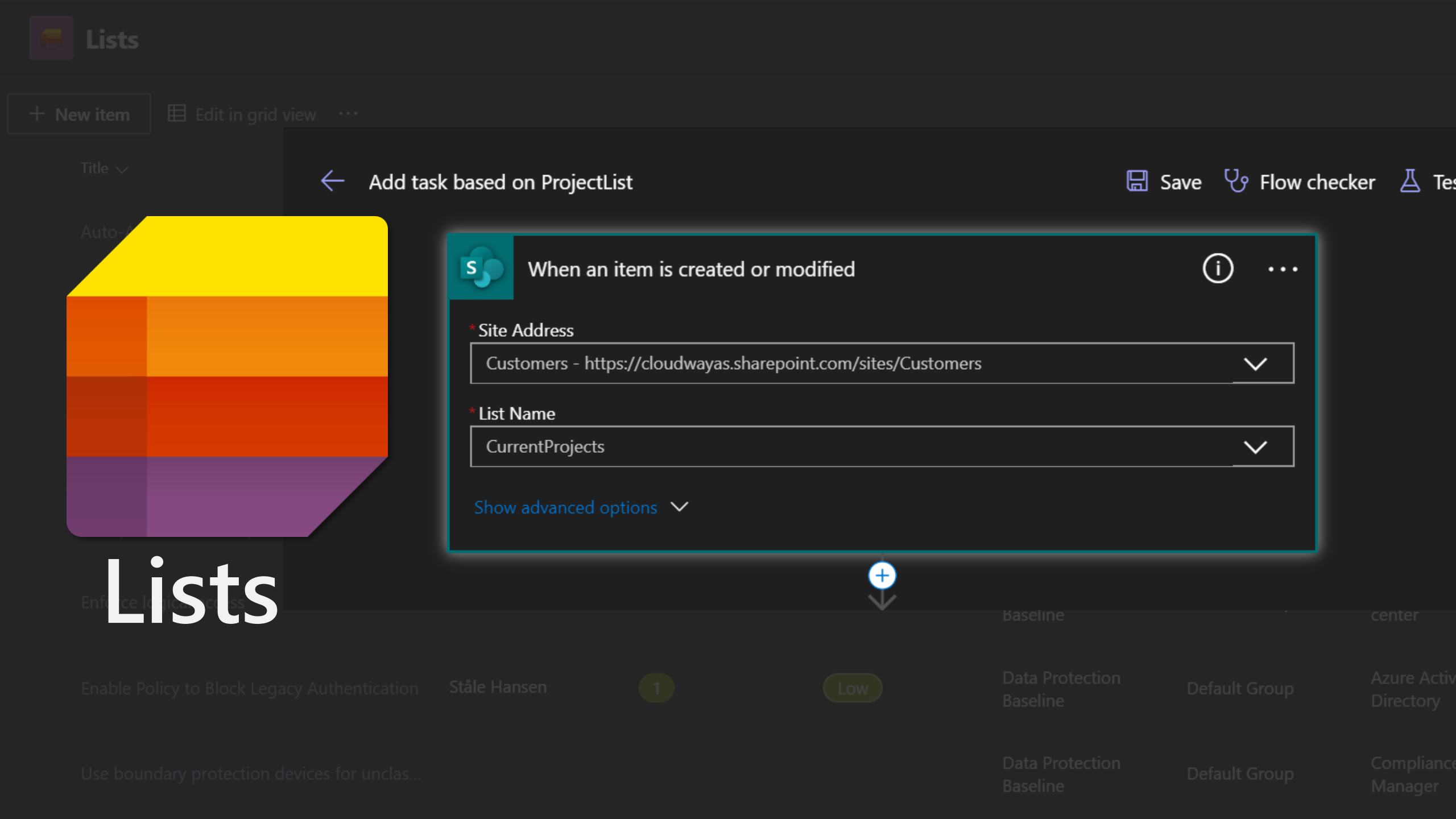
Lists

+ New item | Edit in grid view | ...

Title	Assigned to	Priority	Amount of work	Regulations	Group	Solutions
Auto-Apply Sensitivity Labels	Ståle Hansen	2	High	Data Protection Baseline	Default Group	Information protection
Automate account management	My Buddy	1	Medium	Data Protection Baseline	Default Group	Compliance Manager
Enable Multi-factor Authentication for Non...	Ståle Hansen	1	Low	Data Protection Baseline	Default Group	Azure Activ Directory
Enforce Multi-Factor Authenticator Registra...	Ståle Hansen	1	Low	Data Protection Baseline	Default Group	Azure Activ Directory
Set up ATP Safe Links policies				Data Protection Baseline	Default Group	Office 365 Threat Prot
Enforce logical access				Data Protection Baseline	Default Group	Microsoft 3 center
Enable Policy to Block Legacy Authentication	Ståle Hansen	1	Low	Data Protection Baseline	Default Group	Azure Activ Directory
Use boundary protection devices for unclas...				Data Protection Baseline	Default Group	Compliance Manager

Lists

Each line is a SharePoint element
Conditional formating
Calculating cells
PowerAutomate trigger


Lists
New item
Edit in grid view
Title
Add task based on ProjectList
Save
Flow checker
When an item is created or modified
Site Address
Customers - https://cloudwayas.sharepoint.com/sites/Customers
List Name
CurrentProjects
Show advanced options
Lists
Enable Policy to Block Legacy Authentication
Ståle Hansen
Low
Data Protection Baseline
Default Group
Azure Active Directory
Use boundary protection devices for unclas...
Data Protection Baseline
Default Group
Compliance Manager


NORDIC
— VIRTUAL SUMMIT —

NORDIC
– VIRTUAL SUMMIT –

Consultant

Microsoft 365

NORDIC
– VIRTUAL SUMMIT –

Consultant

Microsoft 365

Customer

NORDIC
– VIRTUAL SUMMIT –

Customer

2020

Microsoft 365

NORDIC
– VIRTUAL SUMMIT –

Customer

2021

Microsoft 365

NORDIC
– VIRTUAL SUMMIT –

Customer

2022

Microsoft 365

NORDIC
– VIRTUAL SUMMIT –

Customer

2023

Microsoft 365

NORDIC
– VIRTUAL SUMMIT –

225 Message Center since April 2020

Major updates: 71
User Impacts: 126
New Features: 79

NORDIC
– VIRTUAL SUMMIT –

2 Drivers for sustainability

NORDIC
– VIRTUAL SUMMIT –

1 Someone must own the tenant roadmap

This is preferably the customer

NORDIC
— VIRTUAL SUMMIT —

M365 and Azure AD
Admin Tools

Controls for Groups,
Identity, Licenses, Access

Offce 365
Admin Tools

Controls for managing Exchange,
SharePoint and Teams
features

Security & Compliance
Admin Tools

Controls for managing
Security & Compliance
across M365

NORDIC
— VIRTUAL SUMMIT —

M365 and Azure AD
Admin Tools

Controls for Groups,
Identity, Licenses, Access

Offce 365
Admin Tools

Controls for managing Exchange,
SharePoint and Teams
features

Security & Compliance
Admin Tools

Controls for managing
Security & Compliance
across M365

What should you outsource?

NORDIC
– VIRTUAL SUMMIT –

2 Use Secure Score and Compliance Score

406 actions for a secure and compliance tenant

NORDIC
– VIRTUAL SUMMIT –

2 You need admin rights to access the scores

Global administrator
Compliance administrator
Security operator
Security reader
Security administrator
Compliance Data Administrator
Global Reader

NORDIC
— VIRTUAL SUMMIT —

2

hin rights

scores

Microsoft Secure Score

Overview | Improvement actions | History | Metrics & trends

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Export

Applied filters:

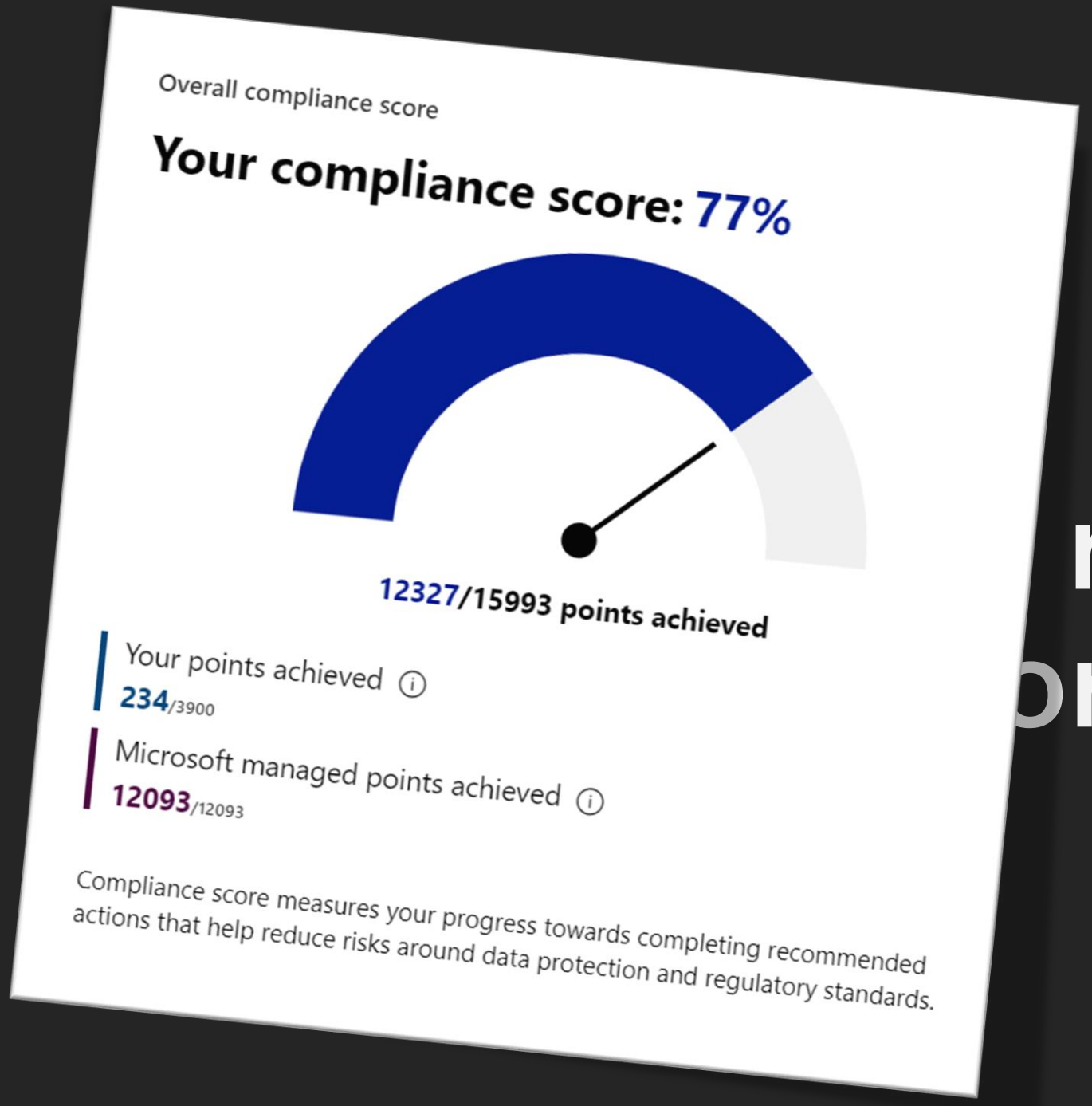
Rank	Improvement action	Score impact	Points achieved	Status	Regressed
128	Disable 'Domain member: Disable machine account password changes'	+0.23%	2/2	Completed	No
129	Turn on customer lockbox feature	+0.11%	1/1	Completed	No
130	Discover trends in shadow IT application usage	+0.11%	1/1	Alternate mitigation	No
131	Designate more than one global admin	+0.11%	1/1	Completed	No
132	Use limited administrative roles	+0.11%	1/1	Completed	No
133	Remove TLS 1.0/1.1 and 3DES dependencies	+0.11%	1/1	Completed	No
134	Fix Advanced Audit Policy issues	+0.11%	1/1	Completed	No
135	Set a honeytoken account	+0.11%	1/1	Alternate mitigation	No
136	Configure VPN integration	+0.11%	1/1	Alternate mitigation	No
137	Configure Microsoft Defender for Endpoint Integration	+0.11%	1/1	Alternate mitigation	No

Points achieved

NORDIC
VIRTUAL SUMMIT

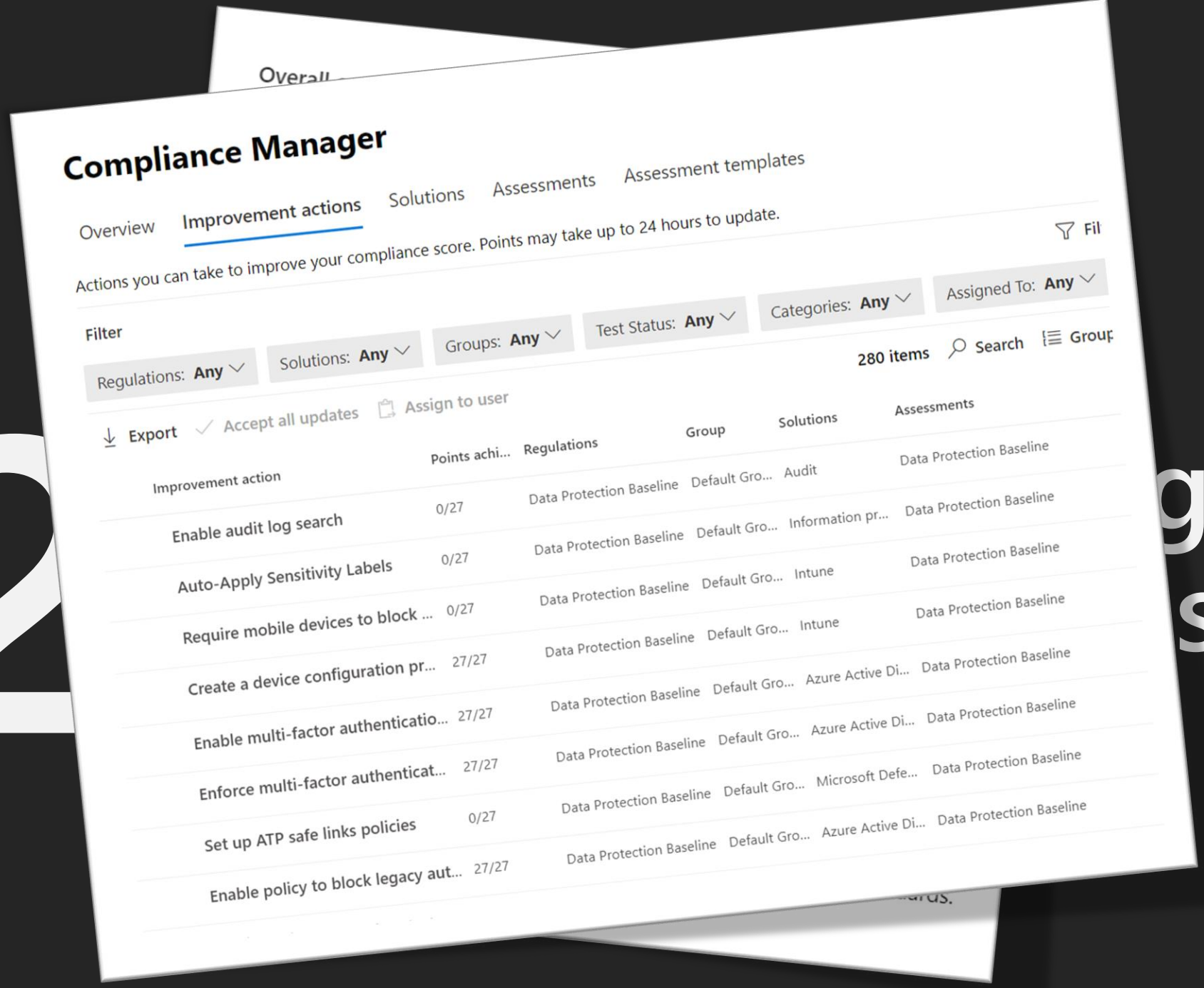
NORDIC
– VIRTUAL SUMMIT –

2



rights

ores



NORDIC
– VIRTUAL SUMMIT –

5 Steps

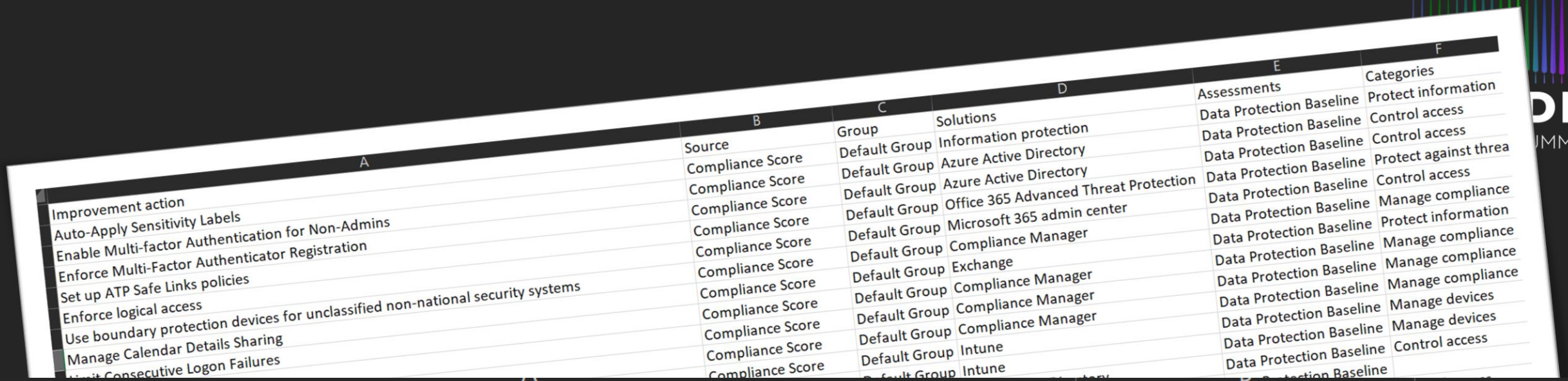
Creating the list

NORDIC
– VIRTUAL SUMMIT –

1 Download the CSV's

Import to excel and add custom columns

	A	B	C	D	E	F
	Improvement action	Source	Group	Solutions	Assessments	Categories
	Auto-Apply Sensitivity Labels	Compliance Score	Default Group	Information protection	Data Protection Baseline	Protect information
	Enable Multi-factor Authentication for Non-Admins	Compliance Score	Default Group	Azure Active Directory	Data Protection Baseline	Control access
	Enforce Multi-Factor Authenticator Registration	Compliance Score	Default Group	Azure Active Directory	Data Protection Baseline	Control access
	Set up ATP Safe Links policies	Compliance Score	Default Group	Office 365 Advanced Threat Protection	Data Protection Baseline	Protect against threa
	Enforce logical access	Compliance Score	Default Group	Microsoft 365 admin center	Data Protection Baseline	Control access
	Use boundary protection devices for unclassified non-national security systems	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	Manage compliance
	Manage Calendar Details Sharing	Compliance Score	Default Group	Exchange	Data Protection Baseline	Protect information
	Limit Consecutive Logon Failures	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	Manage compliance
0	Manage cryptographic keys	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	Manage compliance
1	Establish authenticator types and processes	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	Manage compliance
2	Disallow Simple Passwords on Mobile Devices	Compliance Score	Default Group	Intune	Data Protection Baseline	Manage devices
3	Require Mobile Devices to Have Minimum Password Length	Compliance Score	Default Group	Intune	Data Protection Baseline	Manage devices
4	Restrict access to private keys	Compliance Score	Default Group	Azure Active Directory	Data Protection Baseline	Control access
5	Refresh authenticators	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	
6	Enforce password complexity	Compliance Score	Default Group	Azure Active Directory	Data Protection Baseline	Control access
7	Implement spam filter	Compliance Score	Default Group	Exchange Online Protection	Data Protection Baseline	Protect information
8	Use automated tools to determine password strength	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	Manage compliance
9	Create customized DLP policies for personal data	Compliance Score	Default Group	Data loss prevention	Data Protection Baseline	Protect information
0	Anonymize Usage Activity Reports	Compliance Score	Default Group	Power BI	Data Protection Baseline	Discover and respon
1	Apply sensitivity labels to protect sensitive or critical data	Compliance Score	Default Group	Microsoft Information Protection	Data Protection Baseline	Protect information
2	Activate Azure Rights Management	Compliance Score	Default Group	Azure Information Protection	Data Protection Baseline	Protect information
3	Require Mobile Devices to Use Encryption	Compliance Score	Default Group	Intune	Data Protection Baseline	Manage devices
4	Create a compliance policy for Android enterprise devices	Compliance Score	Default Group	Intune	Data Protection Baseline	Manage devices
5	Enforce rules of behavior and access agreements	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	Manage compliance
6	Create a device configuration profile for Android enterprise devices	Compliance Score	Default Group	Intune	Data Protection Baseline	Manage devices
7	Implement Replay Resistant Authentication Mechanisms - Privileged Accounts	Compliance Score	Default Group	Azure Active Directory	Data Protection Baseline	Control access



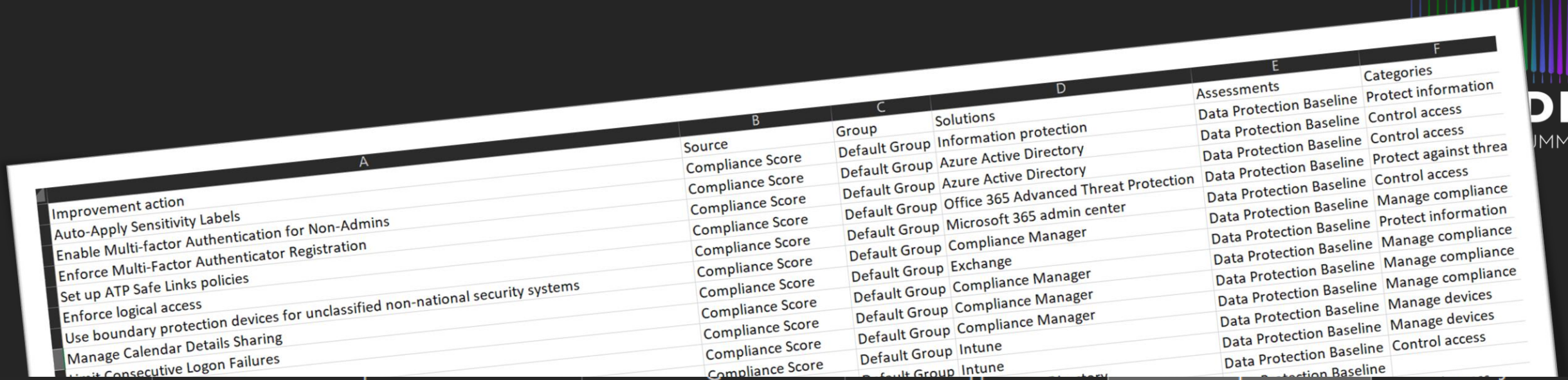
Improvement action	Source	Group	Solutions	Assessments	Categories
Auto-Apply Sensitivity Labels	Compliance Score	Default Group	Information protection	Data Protection Baseline	Protect information
Enable Multi-factor Authentication for Non-Admins	Compliance Score	Default Group	Azure Active Directory	Data Protection Baseline	Control access
Enforce Multi-Factor Authenticator Registration	Compliance Score	Default Group	Azure Active Directory	Data Protection Baseline	Control access
Set up ATP Safe Links policies	Compliance Score	Default Group	Office 365 Advanced Threat Protection	Data Protection Baseline	Protect against threa
Enforce logical access	Compliance Score	Default Group	Microsoft 365 admin center	Data Protection Baseline	Control access
Use boundary protection devices for unclassified non-national security systems	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	Manage compliance
Manage Calendar Details Sharing	Compliance Score	Default Group	Exchange	Data Protection Baseline	Protect information
Limit Consecutive Logon Failures	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	Manage compliance
Apply sensitivity labels to protect sensitive	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	Manage compliance
Activate Azure Rights Management	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	Manage compliance
Require Mobile Devices to Use Encryption	Compliance Score	Default Group	Intune	Data Protection Baseline	Manage devices
Create a compliance policy for Android enterprise devices	Compliance Score	Default Group	Intune	Data Protection Baseline	Manage devices
Enforce rules of behavior and access agreements	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	Control access
Create a device configuration profile for Android enterprise devices	Compliance Score	Default Group	Intune	Data Protection Baseline	
Implement Replay Resistant Authentication Mechanisms - Privileged Accounts	Compliance Score	Default Group	Azure Active Directory	Data Protection Baseline	Control access

Improvement action	Priority	Effort
Auto-Apply Sensitivity Labels	3	high
Enable Multi-factor Authentication for Non-Admins	1	low
Enforce Multi-Factor Authenticator Registration	1	low
Set up ATP Safe Links policies		
Enforce logical access		

Improvement action	Source	Group	Solutions	Assessments	Categories
Auto-Apply Sensitivity Labels	Compliance Score	Default Group	Information protection	Data Protection Baseline	Protect information
Enable Multi-factor Authentication for Non-Admins	Compliance Score	Default Group	Azure Active Directory	Data Protection Baseline	Control access
Enforce Multi-Factor Authenticator Registration	Compliance Score	Default Group	Azure Active Directory	Data Protection Baseline	Control access
Set up ATP Safe Links policies	Compliance Score	Default Group	Office 365 Advanced Threat Protection	Data Protection Baseline	Protect against threa
Enforce logical access	Compliance Score	Default Group	Microsoft 365 admin center	Data Protection Baseline	Control access
Use boundary protection devices for unclassified non-national security systems	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	Manage compliance
Manage Calendar Details Sharing	Compliance Score	Default Group	Exchange	Data Protection Baseline	Protect information
Limit Consecutive Logon Failures	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	Manage compliance
	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	Manage compliance
	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	Manage compliance
	Compliance Score	Default Group	Intune	Data Protection Baseline	Manage devices
	Compliance Score	Default Group	Intune	Data Protection Baseline	Manage devices
				Data Protection Baseline	Control access
				Data Protection Baseline	

Responsible	Comment	Implementation Status	Test status	Tested date
Person1	Need evaluate E5 licenses and needs	Not Planned	None	
Person2	We believe its implemented, needs va	Implemented	Not Tested	
Person3	Waiting feedback		Could not be detected	
			Could not be detected	
			None	

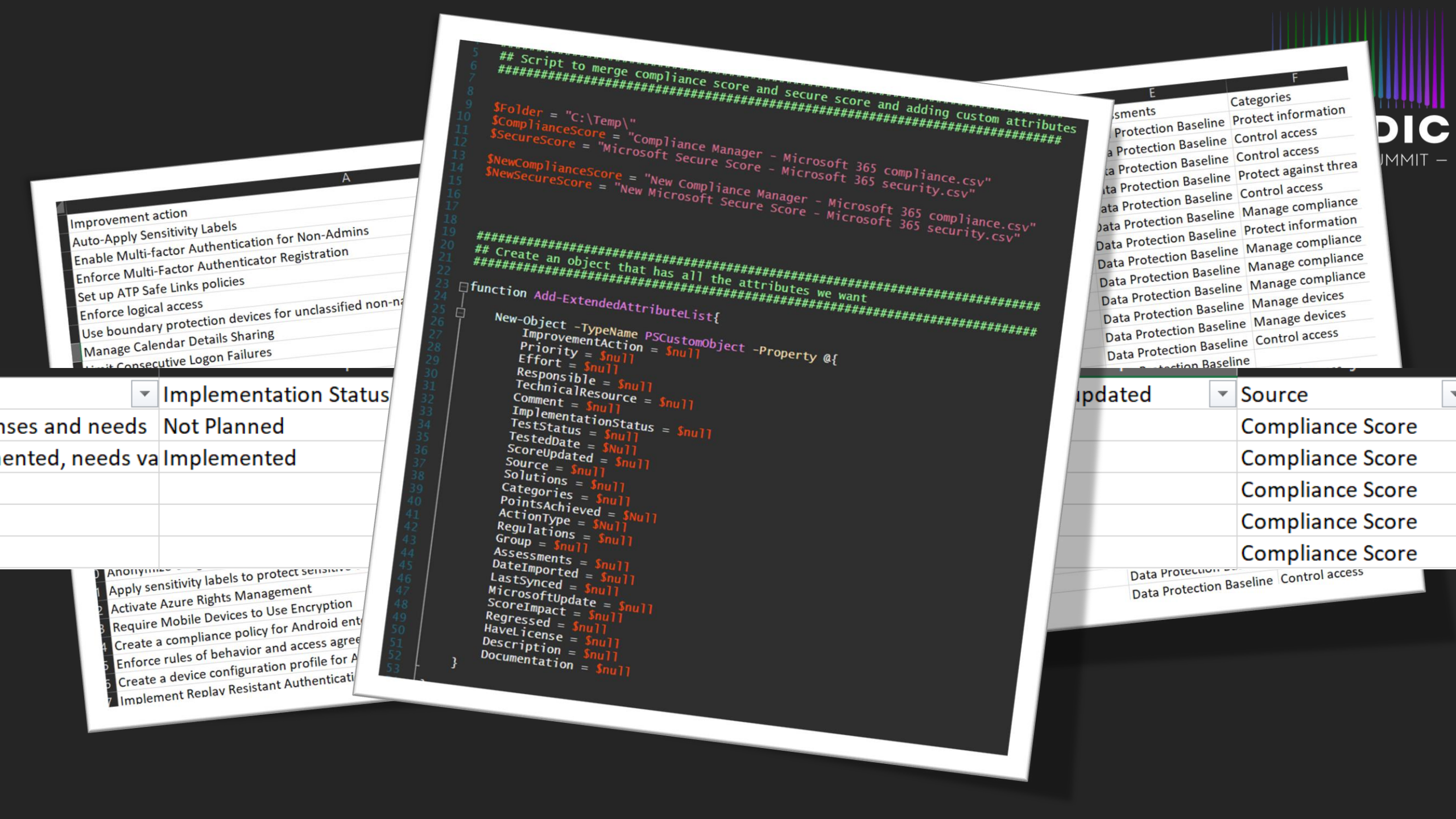
Apply sensitivity labels to protect sensitive	Compliance Score	Default Group	Compliance Manager	Data Protection Ba	
Activate Azure Rights Management	Compliance Score	Default Group	Intune	Data Protection Baseline	Control access
Require Mobile Devices to Use Encryption	Compliance Score	Default Group	Azure Active Directory		
Create a compliance policy for Android enterprise devices	Compliance Score				
Enforce rules of behavior and access agreements					
Create a device configuration profile for Android enterprise devices					
Implement Replay Resistant Authentication Mechanisms - Privileged Accounts					



Improvement action	Source	Group	Solutions	Assessments	Categories
Auto-Apply Sensitivity Labels	Compliance Score	Default Group	Information protection	Data Protection Baseline	Protect information
Enable Multi-factor Authentication for Non-Admins	Compliance Score	Default Group	Azure Active Directory	Data Protection Baseline	Control access
Enforce Multi-Factor Authenticator Registration	Compliance Score	Default Group	Azure Active Directory	Data Protection Baseline	Control access
Set up ATP Safe Links policies	Compliance Score	Default Group	Office 365 Advanced Threat Protection	Data Protection Baseline	Protect against threa
Enforce logical access	Compliance Score	Default Group	Microsoft 365 admin center	Data Protection Baseline	Control access
Use boundary protection devices for unclassified non-national security systems	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	Manage compliance
Manage Calendar Details Sharing	Compliance Score	Default Group	Exchange	Data Protection Baseline	Protect information
Limit Consecutive Logon Failures	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	Manage compliance
	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	Manage compliance
	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	Manage compliance
	Compliance Score	Default Group	Intune	Data Protection Baseline	Manage devices
	Compliance Score	Default Group	Intune	Data Protection Baseline	Manage devices
				Data Protection Baseline	Control access
				Data Protection Baseline	

	Implementation Status	Test status	Tested date	Score updated	Source
nses and needs	Not Planned	None			Compliance Score
ented, needs va	Implemented	Not Tested		No	Compliance Score
		Could not be detected		No	Compliance Score
		Could not be detected			Compliance Score
		None			Compliance Score

Apply sensitivity labels to protect sensitive		Compliance Score	Default Group	Compliance Manager	
Activate Azure Rights Management		Compliance Score	Default Group	Intune	Data Protection Baseline Control access
Require Mobile Devices to Use Encryption		Compliance Score	Default Group	Azure Active Directory	
Create a compliance policy for Android enterprise devices		Compliance Score			
Enforce rules of behavior and access agreements					
Create a device configuration profile for Android enterprise devices					
Implement Replay Resistant Authentication Mechanisms - Privileged Accounts					


Script to merge compliance score and secure score and adding custom attributes
$Folder = "C:\Temp\"
$ComplianceScore = "Compliance Manager - Microsoft 365 compliance.csv"
$SecureScore = "Microsoft Secure Score - Microsoft 365 security.csv"
$NewComplianceScore = "New Compliance Manager - Microsoft 365 compliance.csv"
$NewSecureScore = "New Microsoft Secure Score - Microsoft 365 security.csv"
Create an object that has all the attributes we want
function Add-ExtendedAttributeList{
New-Object -TypeName PSCustomObject -Property @{
ImprovementAction = $null
Priority = $null
Effort = $null
Responsible = $null
TechnicalResource = $null
Comment = $null
ImplementationStatus = $null
TestStatus = $null
TestedDate = $Null
ScoreUpdated = $null
Source = $null
Solutions = $null
Categories = $null
PointsAchieved = $Null
ActionType = $Null
Regulations = $null
Group = $null
Assessments = $null
DateImported = $null
LastSynced = $null
MicrosoftUpdate = $null
ScoreImpact = $null
Regressed = $null
HaveLicense = $null
Description = $null
Documentation = $null
}
A
Improvement action
Auto-Apply Sensitivity Labels
Enable Multi-factor Authentication for Non-Admins
Enforce Multi-Factor Authenticator Registration
Set up ATP Safe Links policies
Enforce logical access
Use boundary protection devices for unclassified non-na
Manage Calendar Details Sharing
E
F
Categories
Protect information
Control access
Control access
Protect against threa
Control access
Manage compliance
Protect information
Manage compliance
Manage compliance
Manage compliance
Manage devices
Manage devices
Control access
Implementation Status
Not Planned
Implemented
Source
Compliance Score
Compliance Score
Compliance Score
Compliance Score
Compliance Score
Apply sensitivity labels to protect
Activate Azure Rights Management
Require Mobile Devices to Use Encryption
Create a compliance policy for Android
Enforce rules of behavior and access
Create a device configuration profile for
Implement Replay Resistant Authenticati
Data Protection Baseline
Control access


#Importing the score csv's
$ComplianceScoreImport = Import-Csv -Path $Folder$ComplianceScore
$SecureScoreImport = Import-Csv -Path $Folder$SecureScore
$CompleteScore = @()
#creating the extended compliance score list
foreach ($Line in $ComplianceScoreImport){
$addObject = Add-ExtendedAttributeList
$addObject.ImprovementAction = $Line.'Improvement action'
$addObject.Source = "Compliance Score"
$addObject.Solutions = $Line.Solutions
$addObject.Categories = $Line.Categories
$addObject.PointsAchieved = $Line.'Points achieved'
$addObject.ActionType = $Line.'Action Type'
$addObject.Group = $Line.Group
$addObject.Assessments = $Line.Assessments
$addObject.DateImported = (Get-Date -Format "yyyy-MM-dd")
$CompleteScore += $addObject
}
#creating the extended secure score list
foreach ($Line in $SecureScoreImport){
$addObject = Add-ExtendedAttributeList
$addObject.ImprovementAction = $Line.'Improvement action'
$addObject.Comment = $Line.Notes
$addObject.Source = "Secure Score"
$addObject.Solutions = $Line.Product
$addObject.Categories = $Line.Categories
$addObject.PointsAchieved = $Line.'Points achieved'
$addObject.ActionType = $Line.'Action Type'
$addObject.Group = $Line.Group
$addObject.Assessments = $Line.Assessments
$addObject.DateImported = (Get-Date -Format "yyyy-MM-dd")
$addObject.LastSynced = $Line.'Last Synced'
$addObject.MicrosoftUpdate = $Line.'Microsoft update'
$addObject.ScoreImpact = $Line.'Score impact'
$addObject.Regressed = $Line.Regressed
$addObject.HaveLicense = $Line.'Have License?'
$addObject.Description = $Line.Description
$addObject.ActionType = "Technical"
$CompleteScore += $addObject
}
$CompleteScore.ImprovementAction
$CompleteScore.Count
$CompleteScore | Select-Object -Property ImprovementAction, Priority, Effort, Responsible, TechnicalResource,
Comment, ImplementationStatus, TestStatus, TestedDate, ScoreUpdated, Source, Solutions, Categories, ActionType,
Regulations, Group, Assessments, DateImported, PointsAchieved, LastSynced, MicrosoftUpdate, ScoreImpact, Regressed,
HaveLicense, Documentation, Description | Export-Csv -Path $Folder"CompleteScore.csv" -NoTypeInformation -Encoding UTF8
Improvement action
Auto-Apply Sensitivity Labels
Enable Multi-factor Authentication
Enforce Multi-Factor Authentication
Set up ATP Safe Links policies
Enforce logical access
Use boundary protection devices
Manage Calendar Details Sharing
Limit Consecutive Logon Failures
E
F
Categories
Protect information
Control access
Control access
Protect against threa
Control access
Manage compliance
Protect information
Manage compliance
Manage compliance
Manage compliance
Manage devices
Manage devices
Control access
Implementa
nses and needs
Not Planned
ented, needs va
Implemented
Source
Compliance Score
Compliance Score
Compliance Score
Compliance Score
Compliance Score
Apply sensitivity labels to protect
Activate Azure Rights Management
Require Mobile Devices to Use En
Create a compliance policy for An
Enforce rules of behavior and acc
Create a device configuration pro
Implement Replay Resistant Auth
Control access

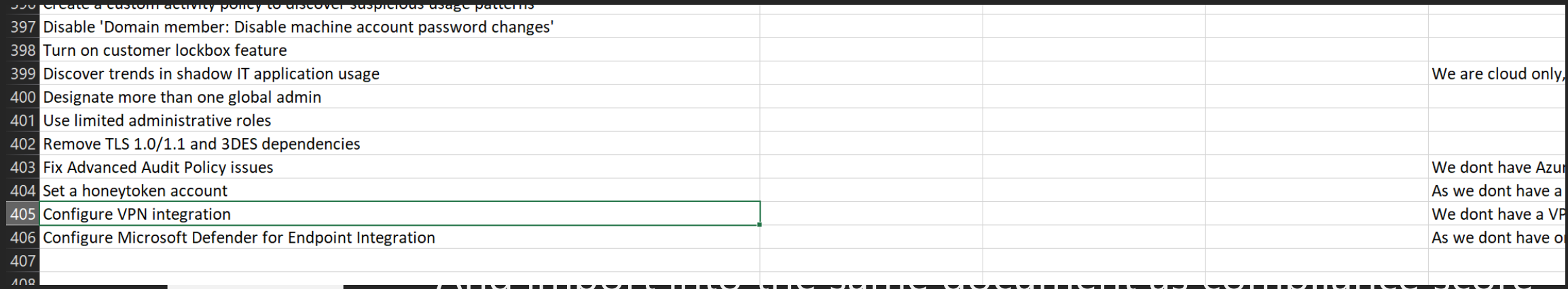

#By Stale Hansen, Twitter: @StaleHansen
Script to merge compliance score and secure score and adding custom attributes
$Folder = "C:\Temp\"
$ComplianceScore = "Compliance Manager - Microsoft 365 compliance.csv"
$SecureScore = "Microsoft Secure Score - Microsoft 365 security.csv"
$NewComplianceScore = "New Compliance Manager - Microsoft 365 compliance.csv"
$NewSecureScore = "New Microsoft Secure Score - Microsoft 365 security.csv"
Create an object that has all the attributes we want
function Add-ExtendedAttributeList{...}
Immport the scores and create the complete score list
#Importing the score csv's
$ComplianceScoreImport = Import-Csv -Path $Folder$ComplianceScore
$SecureScoreImport = Import-Csv -Path $Folder$SecureScore
$CompleteScore = @()
#creating the extended compliance score list
foreach ($Line in $ComplianceScoreImport){...}
#creating the extended secure score list
foreach ($Line in $SecureScoreImport){...}
$CompleteScore.ImprovementAction
$CompleteScore.Count
$CompleteScore | Select-Object -Property ImprovementAction, Priority, Effort, Responsible, TechnicalResource, Comment, ImplementationStatus, TestStatus, TestedDate, ScoreUpdated, Source, Solutions, Categories, ActionType, Regulations, Group, Assessments, DateImported, PointsAchieved, LastSynced, MicrosoftUpdate, ScoreImpact, Regressed, HaveLicense, Documentation, Description | Export-Csv -Path $Folder"CompleteScore.csv" -NoTypeInformation -Encoding UTF8
PS C:\Temp>


#By Stale Hansen, Twitter: @StaleHansen
https://github.com/StaleHansen/Public

NORDIC
– VIRTUAL SUMMIT –

2 Adjust Secure Score CSV

And import into the same document as compliance score



397	Disable 'Domain member: Disable machine account password changes'				
398	Turn on customer lockbox feature				
399	Discover trends in shadow IT application usage				We are cloud only,
400	Designate more than one global admin				
401	Use limited administrative roles				
402	Remove TLS 1.0/1.1 and 3DES dependencies				
403	Fix Advanced Audit Policy issues				We dont have Azu
404	Set a honeytoken account				As we dont have a
405	Configure VPN integration				We dont have a VP
406	Configure Microsoft Defender for Endpoint Integration				As we dont have o
407					

```powershell
#By Ståle Hansen, Twitter: @StaleHansen

#####################################################################################
## Script to merge compliance score and secure score and adding custom attributes
#####################################################################################


$Folder = "C:\Temp\"
$ComplianceScore = "Compliance Manager - Microsoft 365 compliance.csv"
$SecureScore = "Microsoft Secure Score - Microsoft 365 security.csv"

$NewComplianceScore = "New Compliance Manager - Microsoft 365 compliance.csv"
$NewSecureScore = "New Microsoft Secure Score - Microsoft 365 security.csv"



#####################################################################################
## Create an object that has all the attributes we want
#####################################################################################

function Add-ExtendedAttributeList{...}

#####################################################################################
## Immport the scores and create the complete score list
#####################################################################################

#Importing the score csv's
$ComplianceScoreImport = Import-Csv -Path $Folder$ComplianceScore
$SecureScoreImport = Import-Csv -Path $Folder$SecureScore

$CompleteScore = @()

#creating the extended compliance score list
    foreach ($Line in $ComplianceScoreImport){...}

#creating the extended secure score list
    foreach ($Line in $SecureScoreImport){...}

$CompleteScore.ImprovementAction
$CompleteScore.Count

$CompleteScore | Select-Object -Property ImprovementAction, Priority, Effort, Responsible, TechnicalResource, `
Comment, ImplementationStatus, TestStatus, TestedDate, ScoreUpdated, Source, Solutions, Categories, ActionType, `
Regulations, Group, Assessments, DateImported, PointsAchieved, LastSynced, MicrosoftUpdate, ScoreImpact, Regressed, `
HaveLicense, Documentation, Description | Export-Csv -Path $Folder"CompleteScore.csv" -NoTypeInformation -Encoding UTF8
```

```
PS C:\Temp>
```

397	Disable 'Domain member: Disable ma	
398	Turn on customer lockbox feature	
399	Discover trends in shadow IT applicat	We are cloud only,
400	Designate more than one global admi	
401	Use limited administrative roles	
402	Remove TLS 1.0/1.1 and 3DES depen	
403	Fix Advanced Audit Policy issues	We dont have Azu
404	Set a honeytoken account	As we dont have a
405	Configure VPN integration	We dont have a VP
406	Configure Microsoft Defender for E	As we dont have o
407		

NORDIC
— VIRTUAL SUMMIT —

NORDIC
– VIRTUAL SUMMIT –

3 Format as table

And import into Microsoft Lists

NORDIC
— VIRTUAL SUMMIT —

File Home Insert Page Layout Formulas Data Review View Help

Paste Cut Copy Format Painter — Clipboard

Calibri 11 — Font

Wrap Text Merge & Center — Alignment

General — Number

Conditional Formatting

Format as Table

Normal Bad Good
Check Cell Explanatory ... Input

A5 Set up ATP Safe Links policies

Light

White, Table Style Light 1

Medium

NORDIC
– VIRTUAL SUMMIT –

File Home Insert Page Layout

Cut
Copy
Format Painter
Paste
Clipboard

Calibri
B I U
Font

A5
Set up

4 - Operati... Posts Operations 8 more

Welcome to Lists

Create a list
Create a new list for this tab

Add an existing list
Add an existing list to this tab

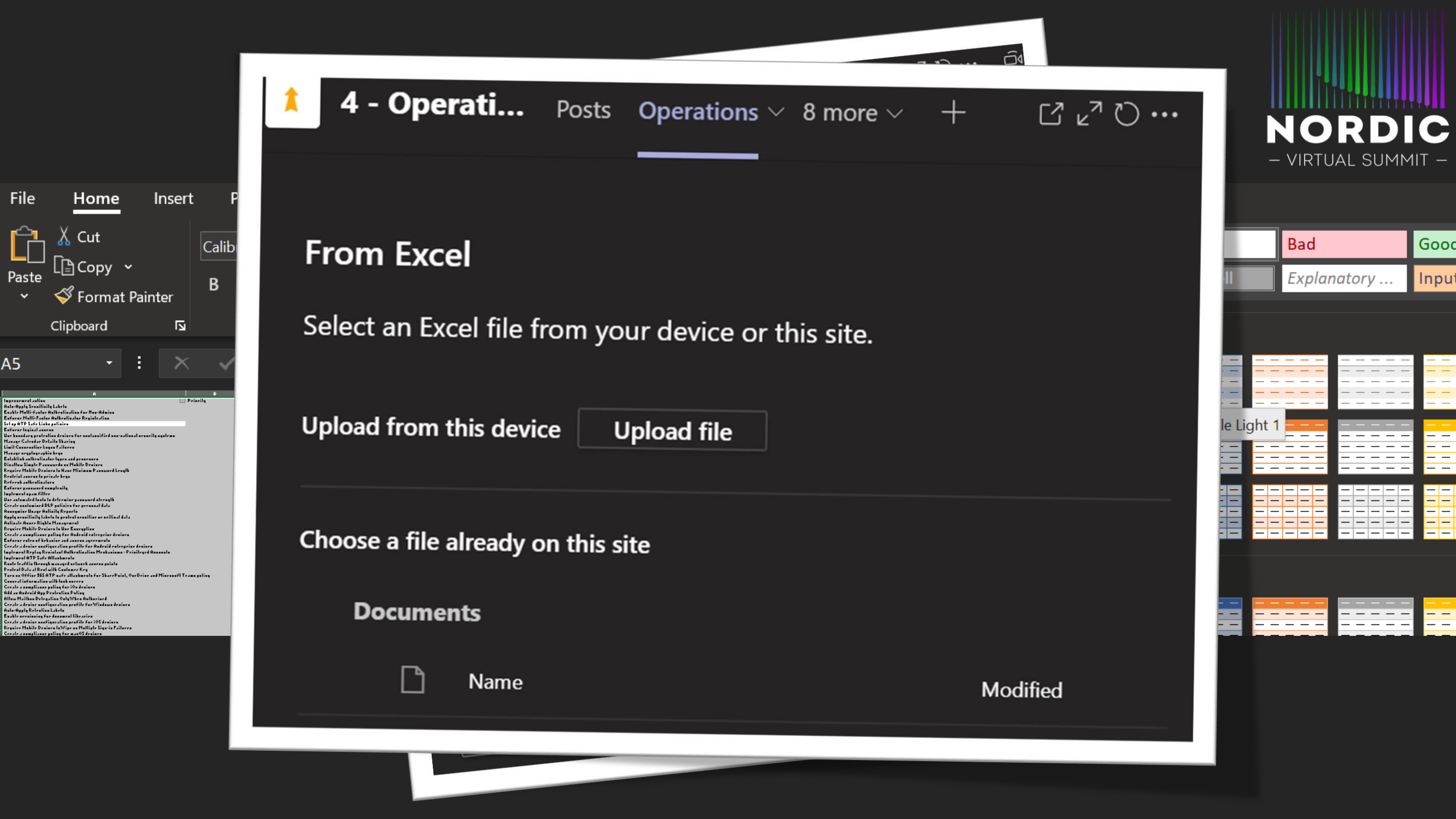
Format as Table

Normal Bad Good
Check Cell Explanatory ... Input

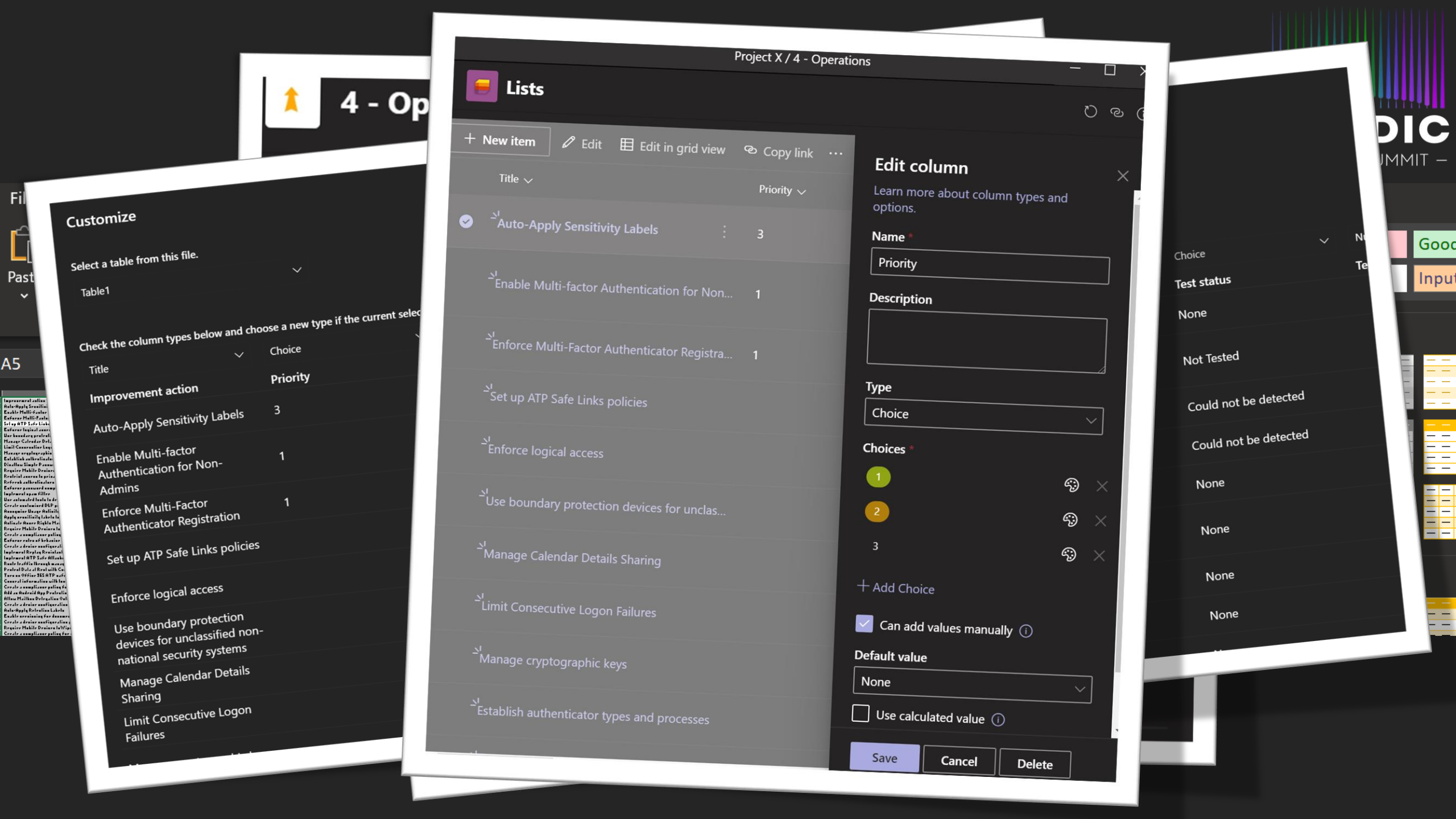
Light

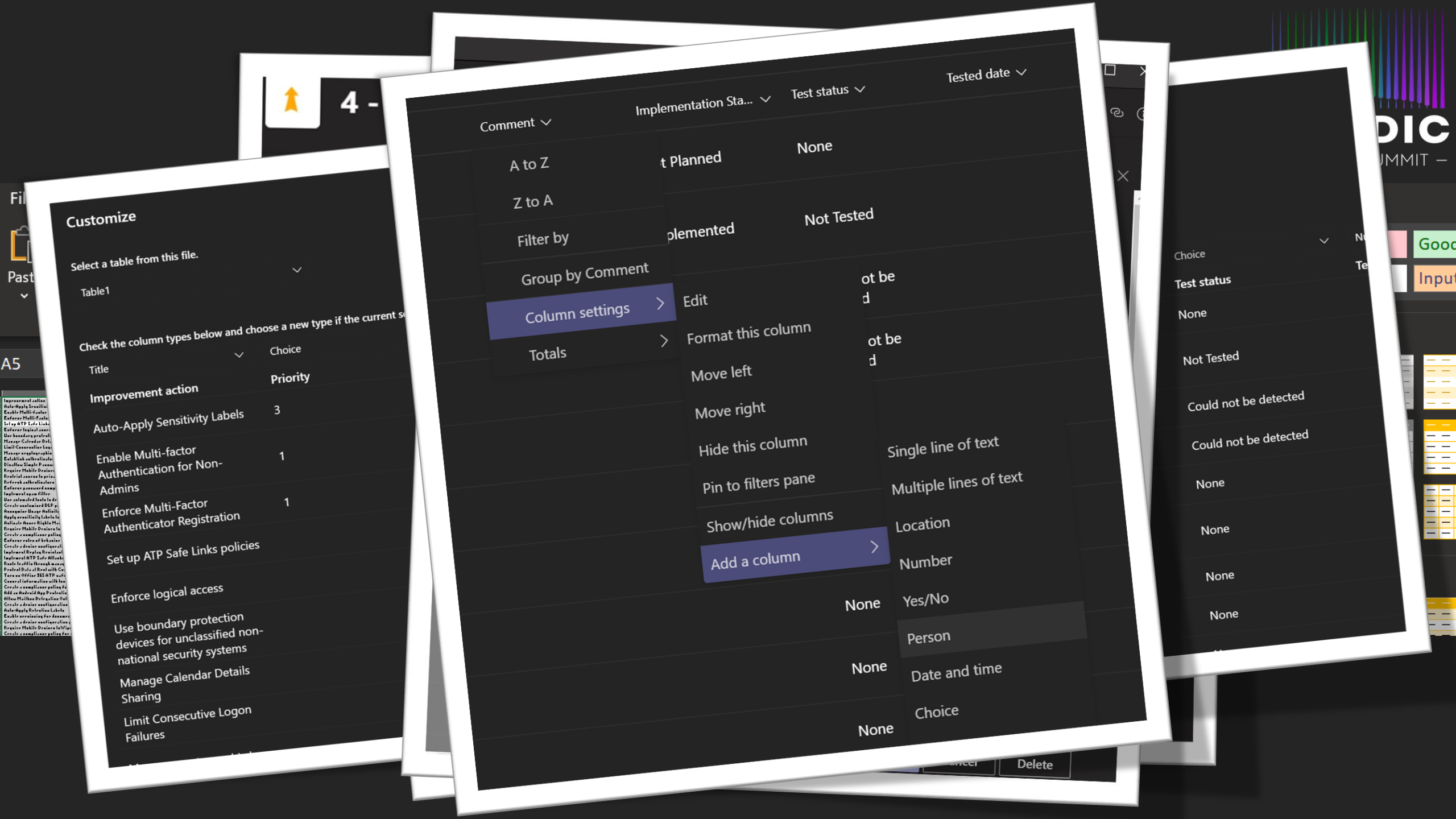
White, Table Style Light 1

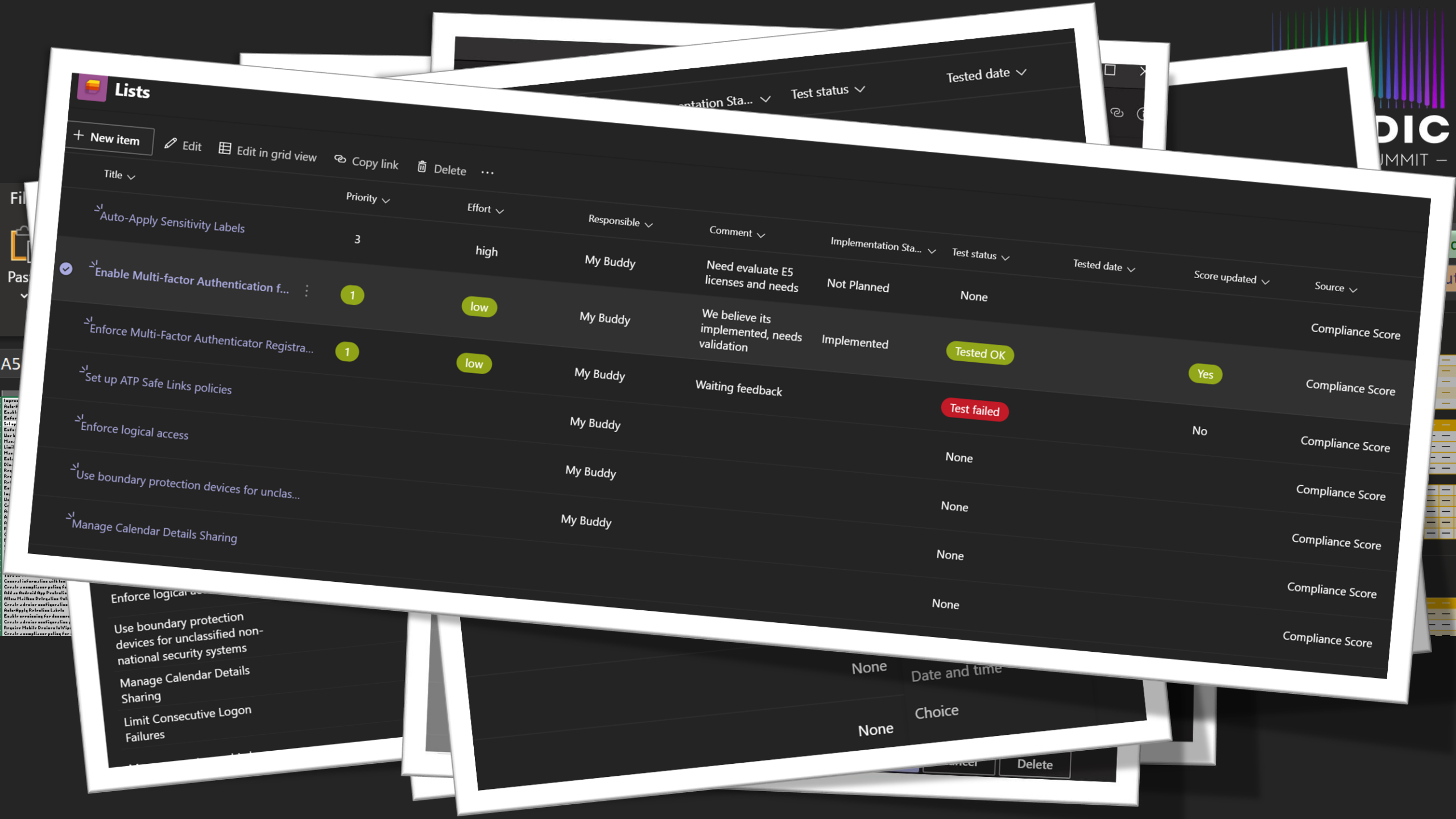
Medium


4 - Operati...
Posts
Operations
8 more
From Excel
Select an Excel file from your device or this site.
Upload from this device
Upload file
Choose a file already on this site
Documents
Name
Modified
File
Home
Insert
Cut
Copy
Format Painter
Paste
Clipboard
A5
Bad
Explanatory ...
NORDIC
VIRTUAL SUMMIT


4 - Operati...
Posts
Customize
Select a table from this file.
Table1
Check the column types below and choose a new type if the current selection is incorrect.
Title
Choice
Choice
Do not import
Single line of text
Choice
Choice
Improvement action
Priority
Effort
Responsible
Comment
Implementation Status
Test status
Auto-Apply Sensitivity Labels
3
high
Person1
Need evaluate E5 licenses and needs
Not Planned
None
Enable Multi-factor Authentication for Non-Admins
1
low
Person2
We believe its implemented, needs validation
Implemented
Not Tested
Enforce Multi-Factor Authenticator Registration
1
low
Person3
Waiting feedback
Could not be detected
Set up ATP Safe Links policies
None
Enforce logical access
None
Use boundary protection devices for unclassified non-national security systems
None
Manage Calendar Details Sharing
None
Limit Consecutive Logon Failures

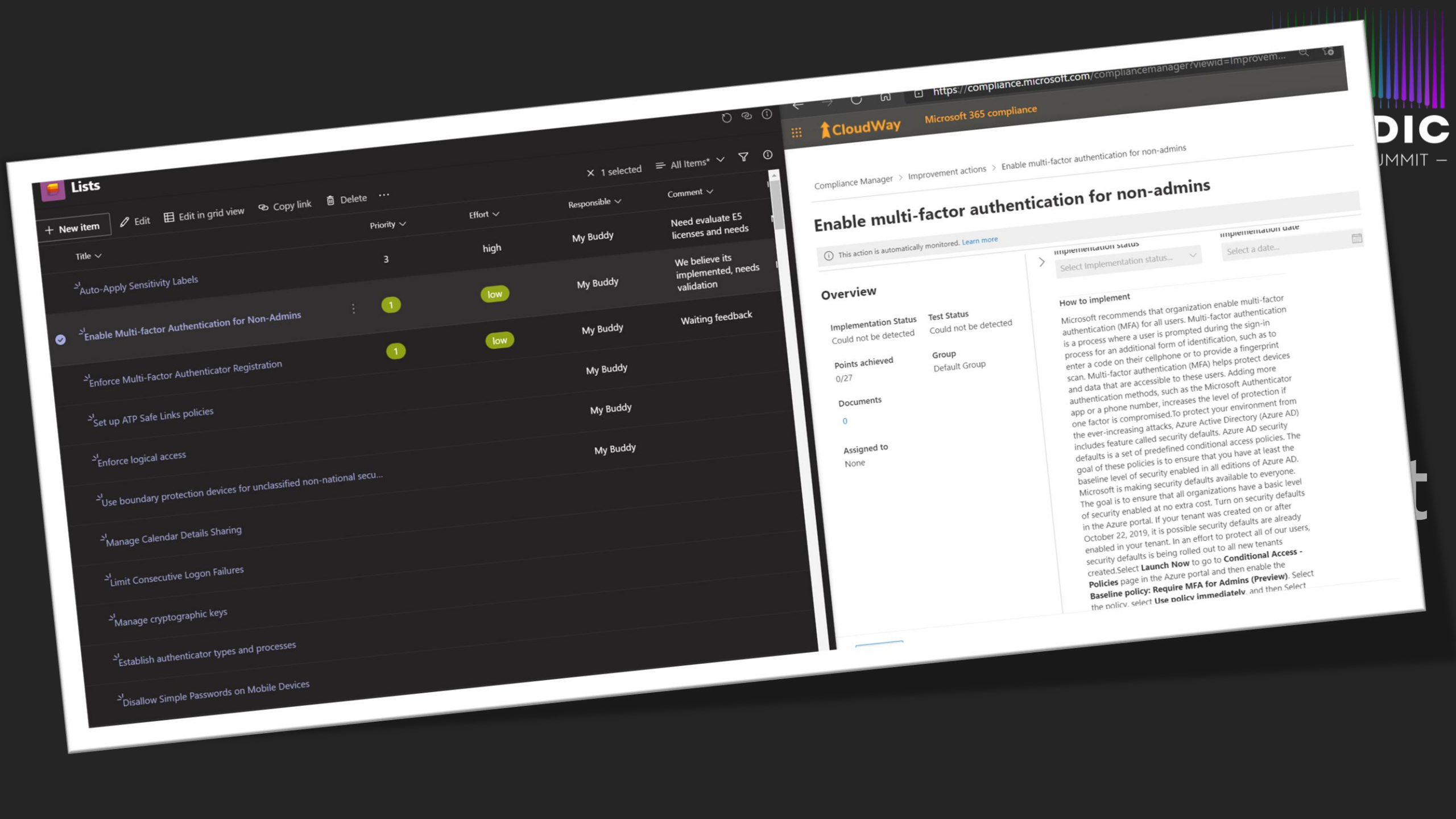

Project X / 4 - Operations
Lists
New item
Edit
Edit in grid view
Copy link
Title
Priority
Auto-Apply Sensitivity Labels 3
Enable Multi-factor Authentication for Non... 1
Enforce Multi-Factor Authenticator Registra... 1
Set up ATP Safe Links policies
Enforce logical access
Use boundary protection devices for unclas...
Manage Calendar Details Sharing
Limit Consecutive Logon Failures
Manage cryptographic keys
Establish authenticator types and processes
Edit column
Learn more about column types and options.
Name *
Priority
Description
Type
Choice
Choices *
1
2
3
Add Choice
Can add values manually
Default value
None
Use calculated value
Save
Cancel
Delete
Customize
Select a table from this file.
Table1
Check the column types below and choose a new type if the current selec
Title
Choice
Improvement action
Priority
Auto-Apply Sensitivity Labels 3
Enable Multi-factor Authentication for Non-Admins 1
Enforce Multi-Factor Authenticator Registration 1
Set up ATP Safe Links policies
Enforce logical access
Use boundary protection devices for unclassified non-national security systems
Manage Calendar Details Sharing
Limit Consecutive Logon Failures
Choice
Test status
None
Not Tested
Could not be detected
Could not be detected
None
None
None
None

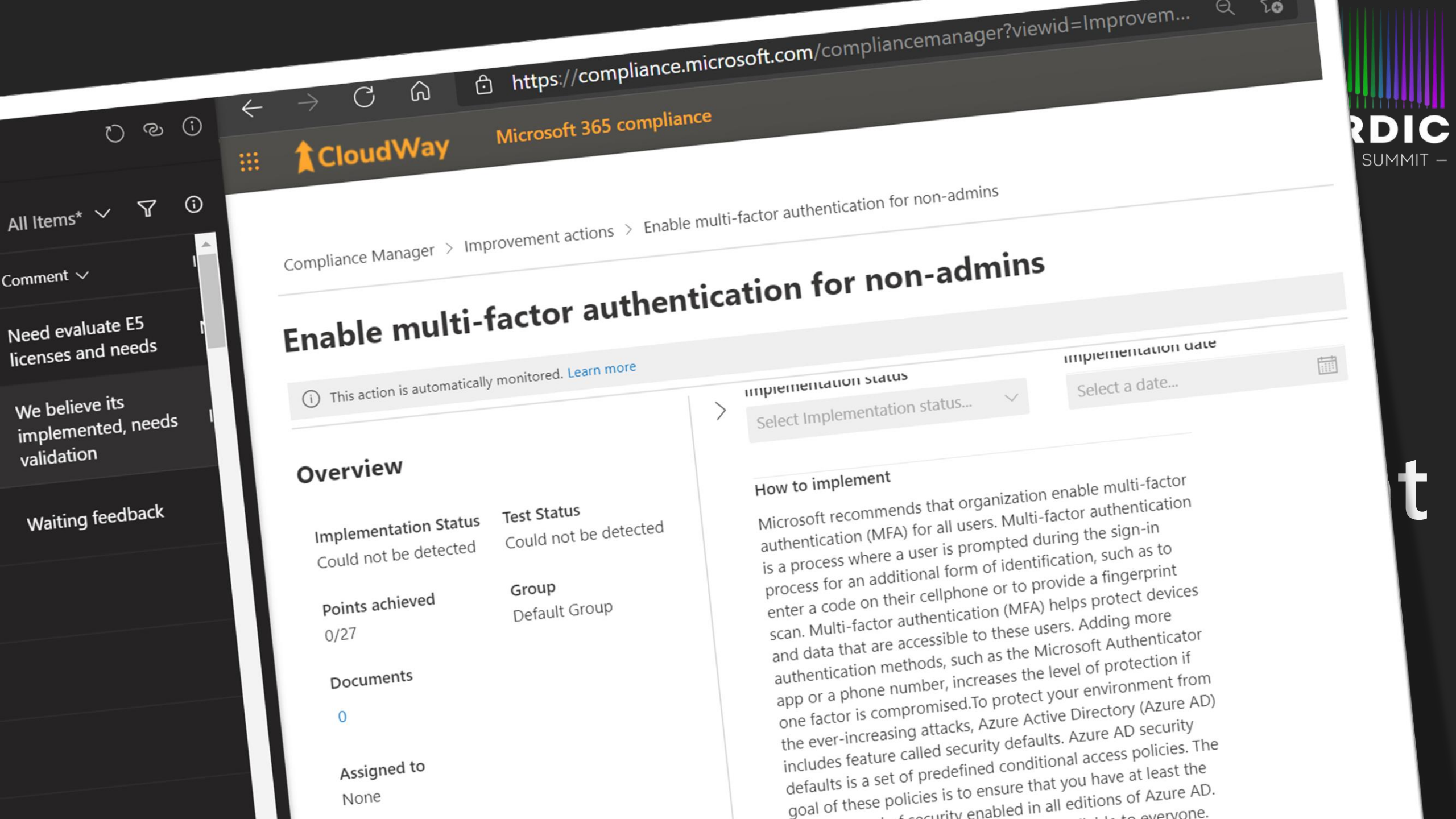

Customize
Select a table from this file.
Table1
Check the column types below and choose a new type if the current s
Title
Choice
Improvement action
Priority
Auto-Apply Sensitivity Labels
3
Enable Multi-factor Authentication for Non-Admins
1
Enforce Multi-Factor Authenticator Registration
1
Set up ATP Safe Links policies
Enforce logical access
Use boundary protection devices for unclassified non-national security systems
Manage Calendar Details Sharing
Limit Consecutive Logon Failures
Comment
Implementation Sta...
Test status
Tested date
A to Z
Z to A
Filter by
Group by Comment
Column settings
Totals
Edit
Format this column
Move left
Move right
Hide this column
Pin to filters pane
Show/hide columns
Add a column
Single line of text
Multiple lines of text
Location
Number
Yes/No
Person
Date and time
Choice
t Planned
None
plemented
Not Tested
ot be
d
ot be
d
None
None
None
Choice
Test status
None
Not Tested
Could not be detected
Could not be detected
None
None
None
None
Delete

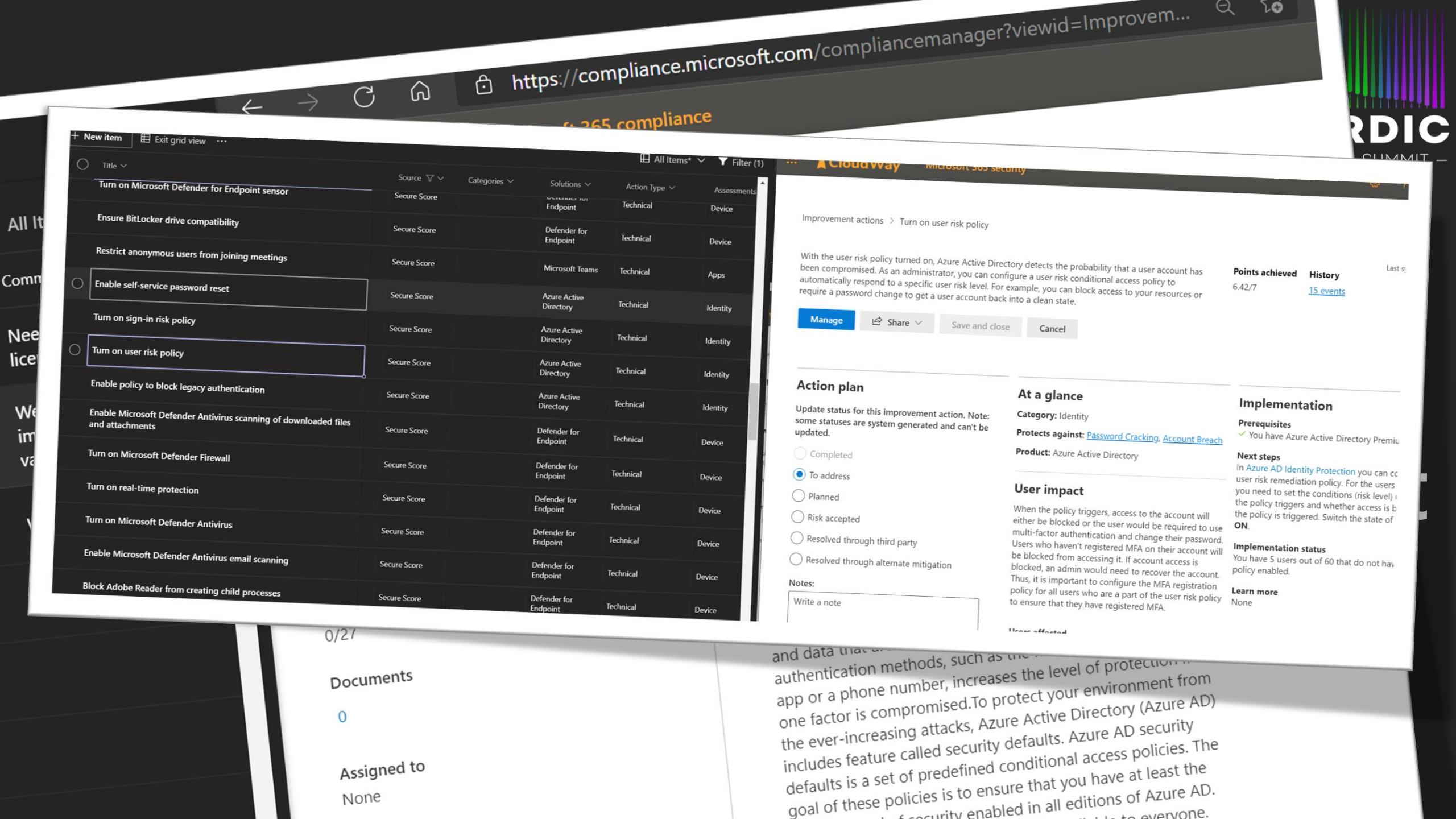

Lists
New item
Edit
Edit in grid view
Copy link
Delete
Title
Priority
Effort
Responsible
Comment
Implementation Sta...
Test status
Tested date
Score updated
Source
Auto-Apply Sensitivity Labels
3
high
My Buddy
Need evaluate E5 licenses and needs
Not Planned
None
Compliance Score
Enable Multi-factor Authentication f...
1
low
My Buddy
We believe its implemented, needs validation
Implemented
Tested OK
Yes
Compliance Score
Enforce Multi-Factor Authenticator Registra...
1
low
My Buddy
Waiting feedback
Test failed
No
Compliance Score
Set up ATP Safe Links policies
My Buddy
None
Compliance Score
Enforce logical access
My Buddy
None
Compliance Score
Use boundary protection devices for unclas...
My Buddy
None
Compliance Score
Manage Calendar Details Sharing
None
Compliance Score
Use boundary protection devices for unclassified non-national security systems
Manage Calendar Details Sharing
Limit Consecutive Logon Failures
None
Date and time
None
Choice
Delete

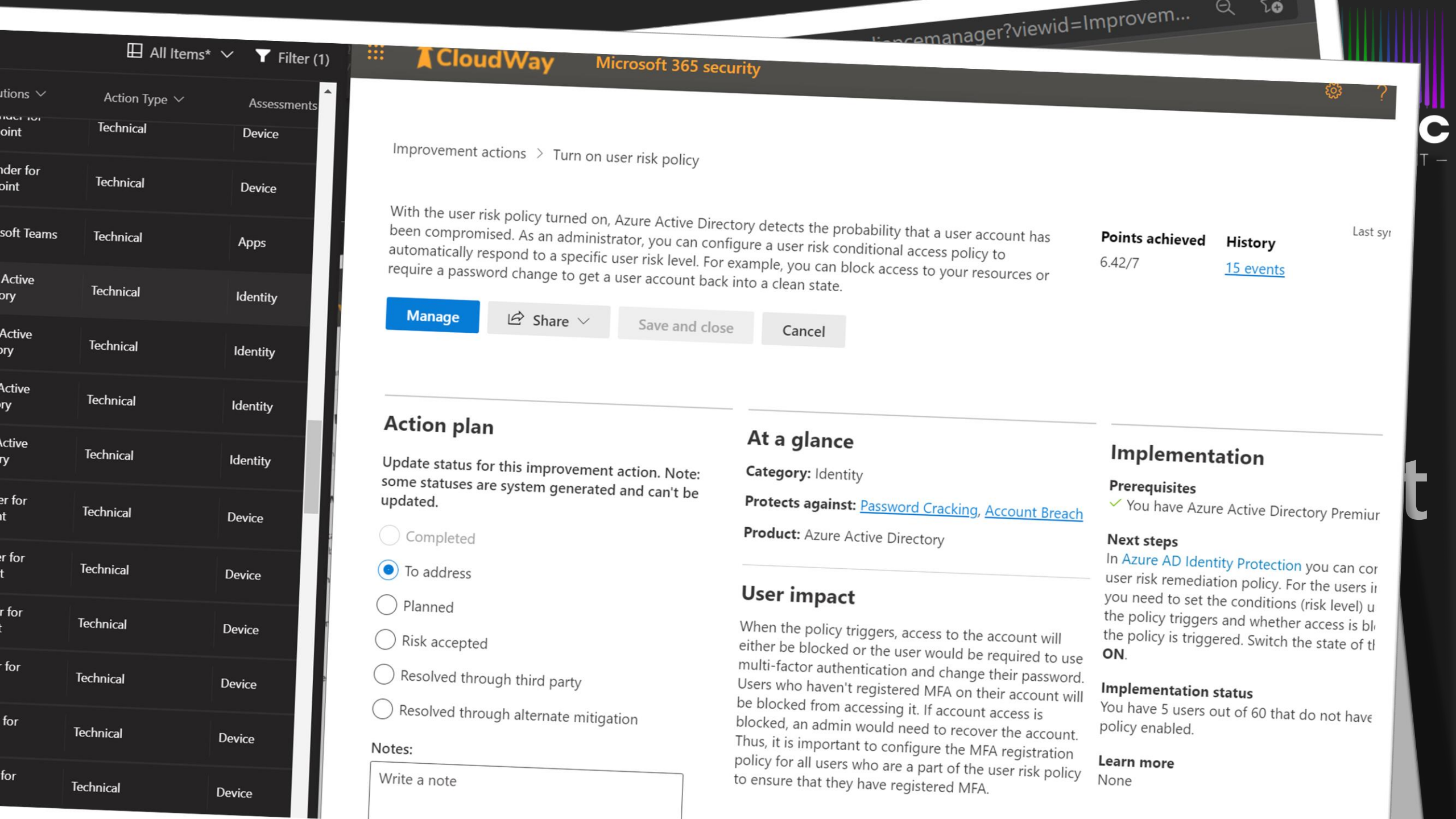
4 Delegate and document

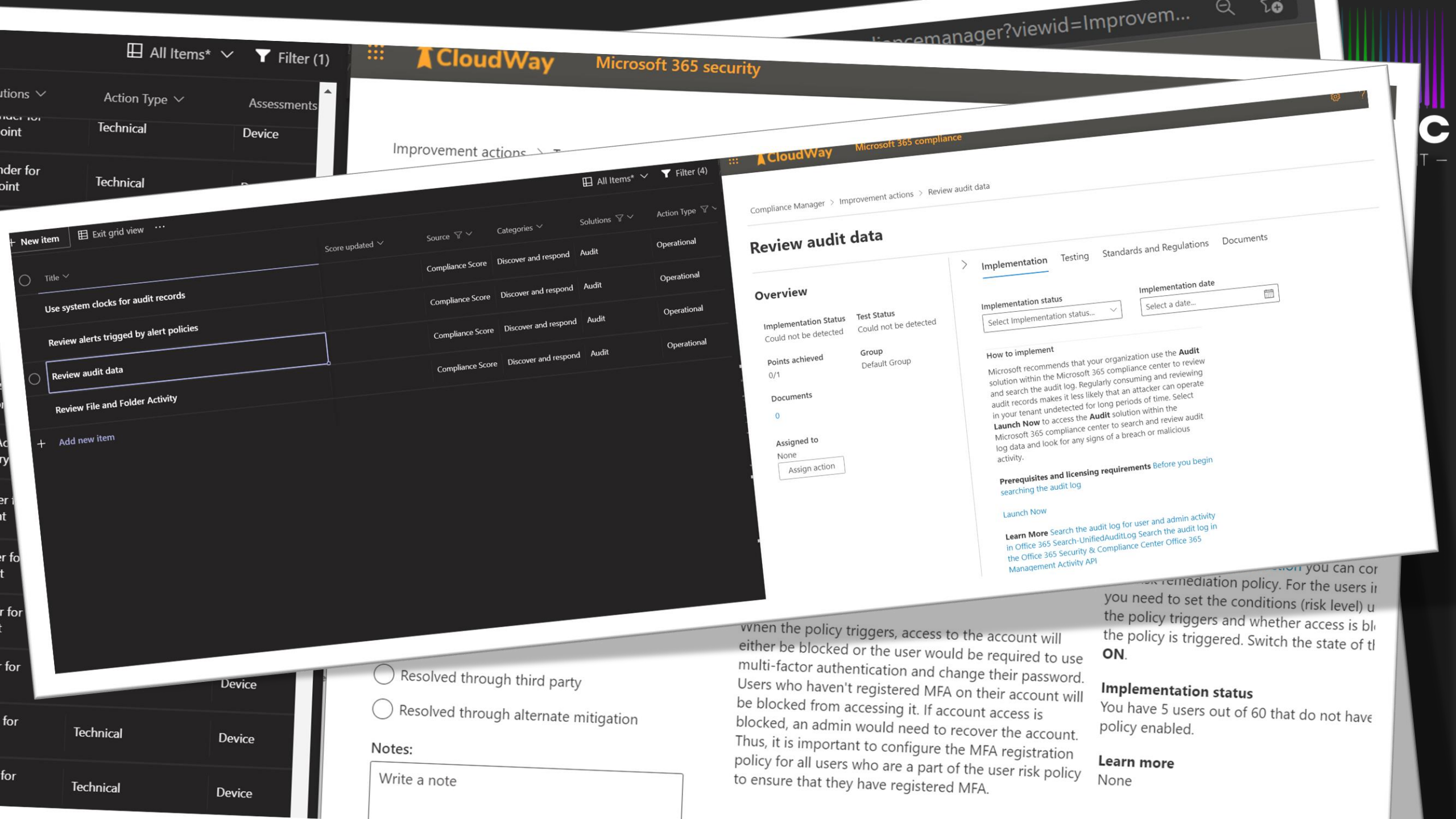
The hard work

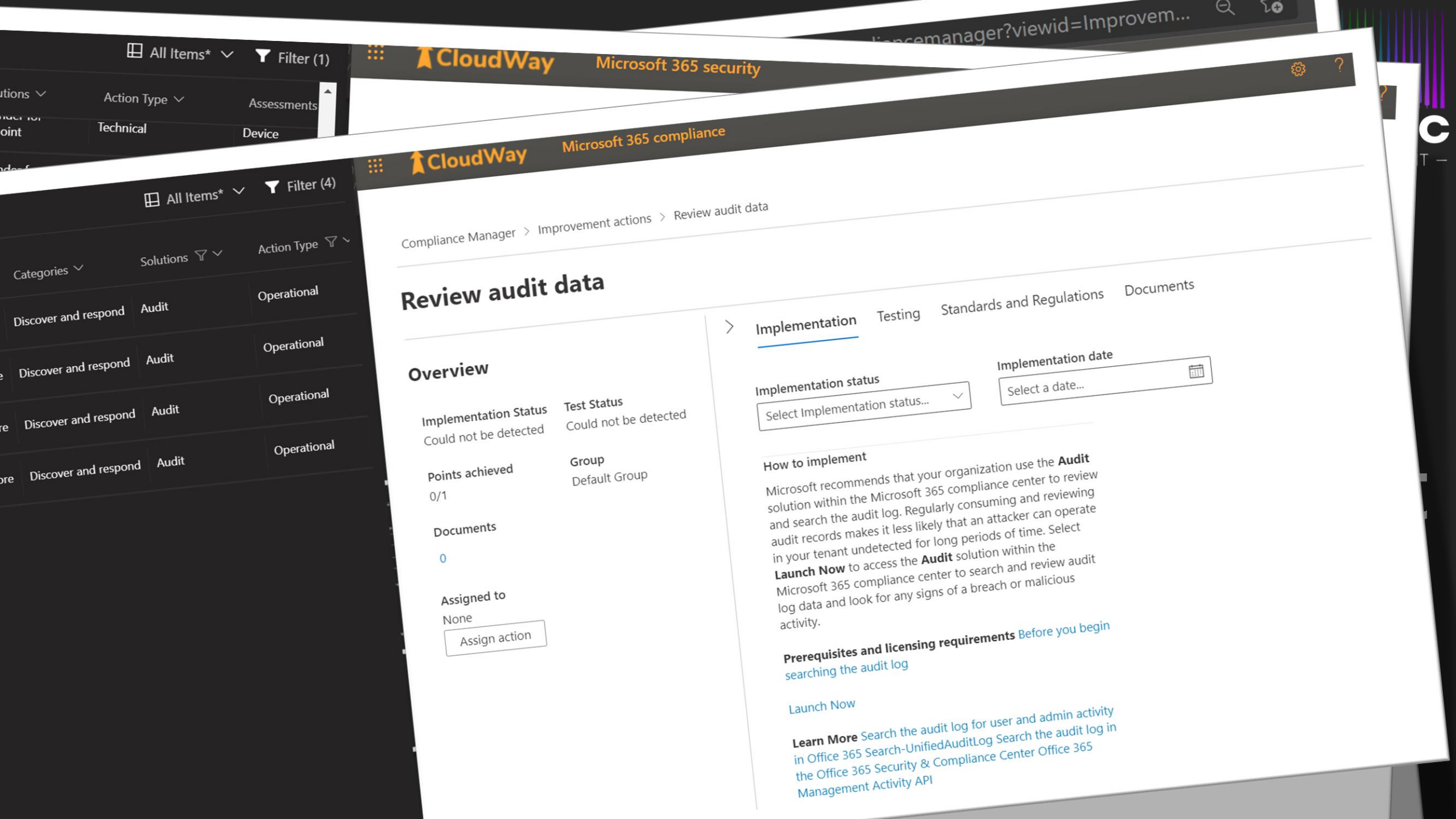

Lists
1 selected
All Items*
New item
Edit
Edit in grid view
Copy link
Delete
Title
Priority
Effort
Responsible
Comment
Auto-Apply Sensitivity Labels
3
high
My Buddy
Need evaluate E5 licenses and needs
Enable Multi-factor Authentication for Non-Admins
1
low
My Buddy
We believe its implemented, needs validation
Enforce Multi-Factor Authenticator Registration
1
low
My Buddy
Waiting feedback
Set up ATP Safe Links policies
My Buddy
Enforce logical access
My Buddy
Use boundary protection devices for unclassified non-national secu...
My Buddy
Manage Calendar Details Sharing
Limit Consecutive Logon Failures
Manage cryptographic keys
Establish authenticator types and processes
Disallow Simple Passwords on Mobile Devices
https://compliance.microsoft.com/compliancemanager?viewid=Improvem...
CloudWay
Microsoft 365 compliance
Compliance Manager
Improvement actions
Enable multi-factor authentication for non-admins
Enable multi-factor authentication for non-admins
This action is automatically monitored. Learn more
Select Implementation status...
Select a date...
Overview
Implementation Status
Could not be detected
Test Status
Could not be detected
Points achieved
0/27
Group
Default Group
Documents
0
Assigned to
None
How to implement
Microsoft recommends that organization enable multi-factor authentication (MFA) for all users. Multi-factor authentication is a process where a user is prompted during the sign-in process for an additional form of identification, such as to enter a code on their cellphone or to provide a fingerprint scan. Multi-factor authentication (MFA) helps protect devices and data that are accessible to these users. Adding more authentication methods, such as the Microsoft Authenticator app or a phone number, increases the level of protection if one factor is compromised.To protect your environment from the ever-increasing attacks, Azure Active Directory (Azure AD) includes feature called security defaults. Azure AD security defaults is a set of predefined conditional access policies. The goal of these policies is to ensure that you have at least the baseline level of security enabled in all editions of Azure AD. Microsoft is making security defaults available to everyone. The goal is to ensure that all organizations have a basic level of security enabled at no extra cost. Turn on security defaults in the Azure portal. If your tenant was created on or after October 22, 2019, it is possible security defaults are already enabled in your tenant. In an effort to protect all of our users, security defaults is being rolled out to all new tenants created.Select Launch Now to go to Conditional Access - Policies page in the Azure portal and then enable the Baseline policy: Require MFA for Admins (Preview). Select the policy, select Use policy immediately, and then Select

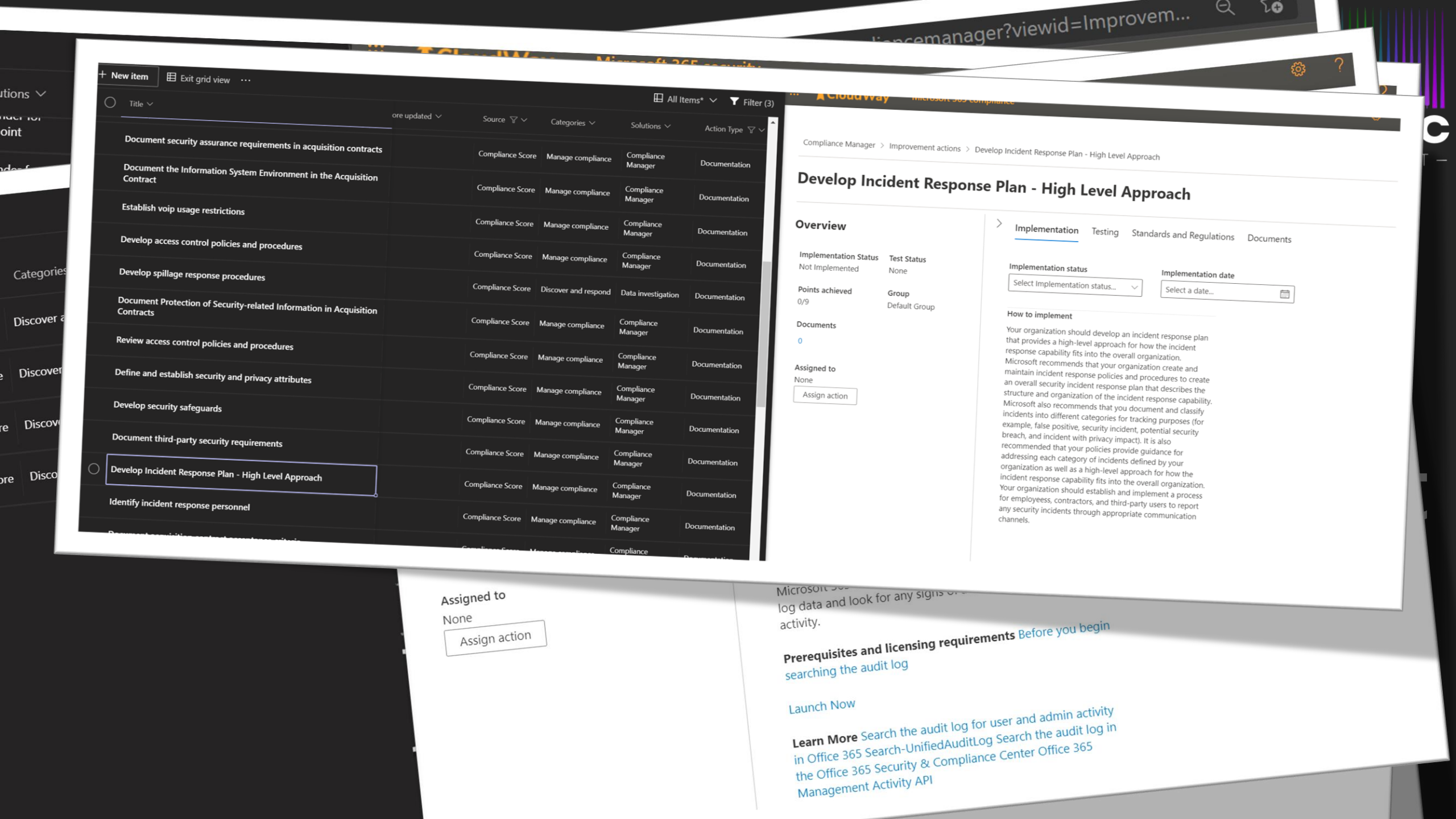

https://compliance.microsoft.com/compliancemanager?viewid=Improvem...
CloudWay
Microsoft 365 compliance
All Items*
Comment
Need evaluate E5 licenses and needs
We believe its implemented, needs validation
Waiting feedback
Compliance Manager > Improvement actions > Enable multi-factor authentication for non-admins
Enable multi-factor authentication for non-admins
This action is automatically monitored. Learn more
Overview
Implementation Status
Could not be detected
Test Status
Could not be detected
Points achieved
0/27
Group
Default Group
Documents
0
Assigned to
None
Implementation status
Select Implementation status...
Implementation date
Select a date...
How to implement
Microsoft recommends that organization enable multi-factor authentication (MFA) for all users. Multi-factor authentication is a process where a user is prompted during the sign-in process for an additional form of identification, such as to enter a code on their cellphone or to provide a fingerprint scan. Multi-factor authentication (MFA) helps protect devices and data that are accessible to these users. Adding more authentication methods, such as the Microsoft Authenticator app or a phone number, increases the level of protection if one factor is compromised.To protect your environment from the ever-increasing attacks, Azure Active Directory (Azure AD) includes feature called security defaults. Azure AD security defaults is a set of predefined conditional access policies. The goal of these policies is to ensure that you have at least the
SUMMIT

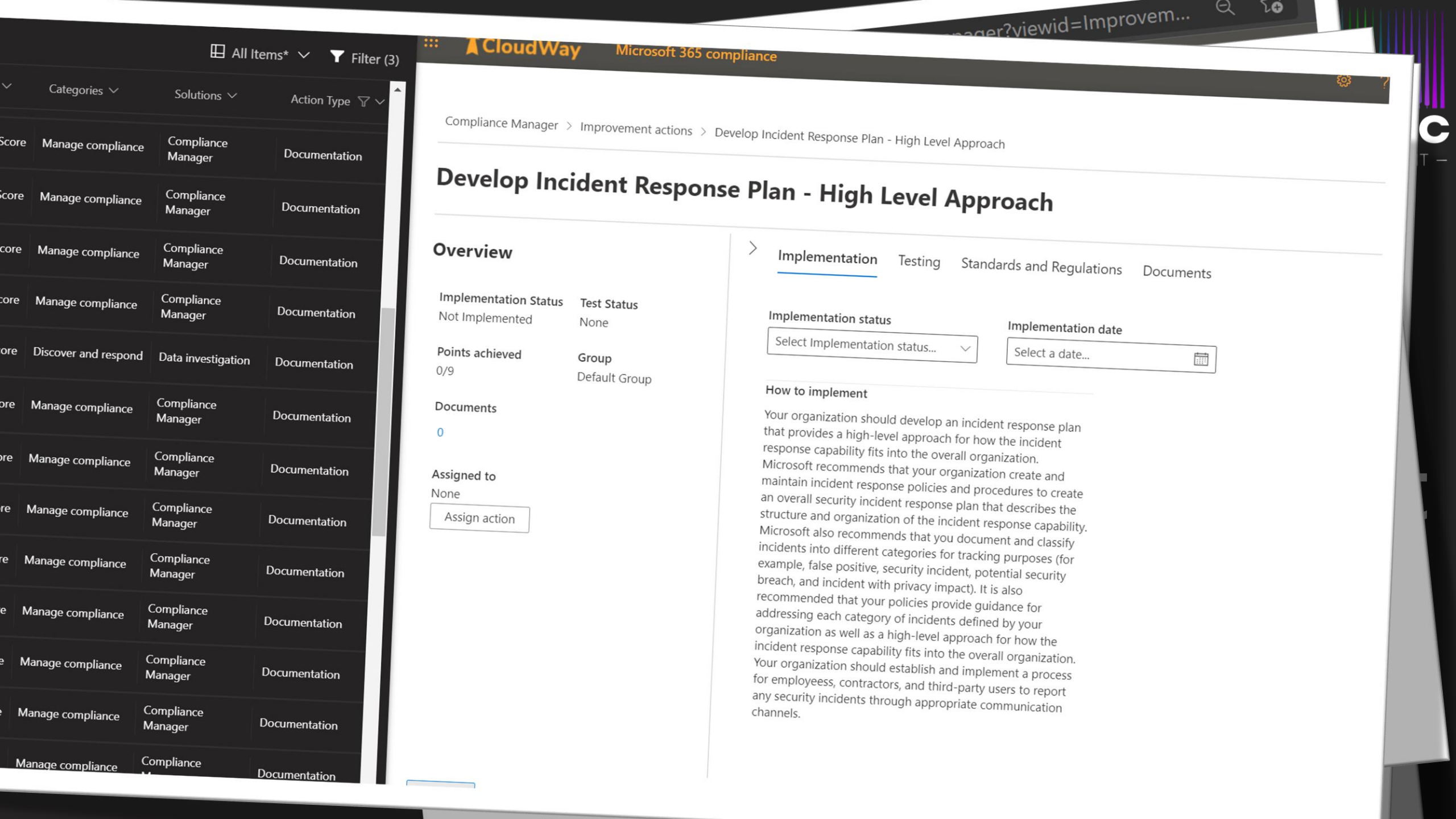

https://compliance.microsoft.com/compliancemanager?viewid=Improvem...
365 compliance
New item
Exit grid view
All Items*
Filter (1)
Title
Source
Categories
Solutions
Action Type
Assessments
Turn on Microsoft Defender for Endpoint sensor
Secure Score
Technical
Device
Ensure BitLocker drive compatibility
Secure Score
Defender for Endpoint
Technical
Device
Restrict anonymous users from joining meetings
Secure Score
Microsoft Teams
Technical
Apps
Enable self-service password reset
Secure Score
Azure Active Directory
Technical
Identity
Turn on sign-in risk policy
Secure Score
Azure Active Directory
Technical
Identity
Turn on user risk policy
Secure Score
Azure Active Directory
Technical
Identity
Enable policy to block legacy authentication
Secure Score
Azure Active Directory
Technical
Identity
Enable Microsoft Defender Antivirus scanning of downloaded files and attachments
Secure Score
Defender for Endpoint
Technical
Device
Turn on Microsoft Defender Firewall
Secure Score
Defender for Endpoint
Technical
Device
Turn on real-time protection
Secure Score
Defender for Endpoint
Technical
Device
Turn on Microsoft Defender Antivirus
Secure Score
Defender for Endpoint
Technical
Device
Enable Microsoft Defender Antivirus email scanning
Secure Score
Defender for Endpoint
Technical
Device
Block Adobe Reader from creating child processes
Secure Score
Defender for Endpoint
Technical
Device
CloudWay
Improvement actions
Turn on user risk policy
With the user risk policy turned on, Azure Active Directory detects the probability that a user account has been compromised. As an administrator, you can configure a user risk conditional access policy to automatically respond to a specific user risk level. For example, you can block access to your resources or require a password change to get a user account back into a clean state.
Points achieved
6.42/7
History
15 events
Manage
Share
Save and close
Cancel
Action plan
Update status for this improvement action. 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
At a glance
Category: Identity
Protects against: Password Cracking, Account Breach
Product: Azure Active Directory
User impact
When the policy triggers, access to the account will either be blocked or the user would be required to use multi-factor authentication and change their password. Users who haven't registered MFA on their account will be blocked from accessing it. If account access is blocked, an admin would need to recover the account. Thus, it is important to configure the MFA registration policy for all users who are a part of the user risk policy to ensure that they have registered MFA.
Implementation
Prerequisites
You have Azure Active Directory Premiu
Next steps
In Azure AD Identity Protection you can cc
user risk remediation policy. For the users
you need to set the conditions (risk level)
the policy triggers and whether access is b
the policy is triggered. Switch the state of
ON.
Implementation status
You have 5 users out of 60 that do not hav
policy enabled.
Learn more
None
0/27
Documents
0
Assigned to
None
authentication methods, such as the
app or a phone number, increases the level of protection
one factor is compromised.To protect your environment from
the ever-increasing attacks, Azure Active Directory (Azure AD)
includes feature called security defaults. Azure AD security
defaults is a set of predefined conditional access policies. The
goal of these policies is to ensure that you have at least the
security enabled in all editions of Azure AD.


All Items*
Filter (1)
Action Type
Assessments
Technical
Device
Technical
Device
Technical
Apps
Technical
Identity
Technical
Identity
Technical
Identity
Technical
Identity
Technical
Device
Technical
Device
Technical
Device
Technical
Device
Technical
Device
Technical
Device
CloudWay
Microsoft 365 security
Improvement actions
Turn on user risk policy
With the user risk policy turned on, Azure Active Directory detects the probability that a user account has been compromised. As an administrator, you can configure a user risk conditional access policy to automatically respond to a specific user risk level. For example, you can block access to your resources or require a password change to get a user account back into a clean state.
Points achieved
6.42/7
History
15 events
Manage
Share
Save and close
Cancel
Action plan
Update status for this improvement action. 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
At a glance
Category: Identity
Protects against: Password Cracking, Account Breach
Product: Azure Active Directory
User impact
When the policy triggers, access to the account will either be blocked or the user would be required to use multi-factor authentication and change their password. Users who haven't registered MFA on their account will be blocked from accessing it. If account access is blocked, an admin would need to recover the account. Thus, it is important to configure the MFA registration policy for all users who are a part of the user risk policy to ensure that they have registered MFA.
Implementation
Prerequisites
You have Azure Active Directory Premiur
Next steps
In Azure AD Identity Protection you can cor
user risk remediation policy. For the users i
you need to set the conditions (risk level) u
the policy triggers and whether access is bl
the policy is triggered. Switch the state of tl
ON.
Implementation status
You have 5 users out of 60 that do not have
policy enabled.
Learn more
None


All Items*
Filter (1)
Action Type
Assessments
Technical
Device
CloudWay
Microsoft 365 security
Improvement actions
All Items*
Filter (4)
New item
Exit grid view
Title
Score updated
Source
Categories
Solutions
Action Type
Use system clocks for audit records
Review alerts trigged by alert policies
Review audit data
Review File and Folder Activity
Add new item
Compliance Score
Discover and respond
Audit
Operational
CloudWay
Microsoft 365 compliance
Compliance Manager
Improvement actions
Review audit data
Review audit data
Overview
Implementation Status
Could not be detected
Test Status
Could not be detected
Points achieved
0/1
Group
Default Group
Documents
0
Assigned to
None
Assign action
Implementation
Testing
Standards and Regulations
Documents
Implementation status
Select Implementation status...
Implementation date
Select a date...
How to implement
Microsoft recommends that your organization use the Audit solution within the Microsoft 365 compliance center to review and search the audit log. Regularly consuming and reviewing audit records makes it less likely that an attacker can operate in your tenant undetected for long periods of time. Select Launch Now to access the Audit solution within the Microsoft 365 compliance center to search and review audit log data and look for any signs of a breach or malicious activity.
Prerequisites and licensing requirements Before you begin searching the audit log
Launch Now
Learn More Search the audit log for user and admin activity in Office 365 Search-UnifiedAuditLog Search the audit log in the Office 365 Security & Compliance Center Office 365 Management Activity API
Resolved through third party
Resolved through alternate mitigation
Notes:
Write a note
When the policy triggers, access to the account will either be blocked or the user would be required to use multi-factor authentication and change their password. Users who haven't registered MFA on their account will be blocked from accessing it. If account access is blocked, an admin would need to recover the account. Thus, it is important to configure the MFA registration policy for all users who are a part of the user risk policy to ensure that they have registered MFA.
you need to set the conditions (risk level) u
the policy triggers and whether access is bl
the policy is triggered. Switch the state of t
ON.
Implementation status
You have 5 users out of 60 that do not have
policy enabled.
Learn more
None


All Items*
Filter (1)
Action Type
Assessments
Technical
Device
CloudWay
Microsoft 365 security
All Items*
Filter (4)
Categories
Solutions
Action Type
Discover and respond
Audit
Operational
Discover and respond
Audit
Operational
Discover and respond
Audit
Operational
Discover and respond
Audit
Operational
CloudWay
Microsoft 365 compliance
Compliance Manager
Improvement actions
Review audit data
Review audit data
Overview
Implementation Status
Could not be detected
Test Status
Could not be detected
Points achieved
0/1
Group
Default Group
Documents
0
Assigned to
None
Assign action
Implementation
Testing
Standards and Regulations
Documents
Implementation status
Select Implementation status...
Implementation date
Select a date...
How to implement
Microsoft recommends that your organization use the Audit solution within the Microsoft 365 compliance center to review and search the audit log. Regularly consuming and reviewing audit records makes it less likely that an attacker can operate in your tenant undetected for long periods of time. Select Launch Now to access the Audit solution within the Microsoft 365 compliance center to search and review audit log data and look for any signs of a breach or malicious activity.
Prerequisites and licensing requirements Before you begin searching the audit log
Launch Now
Learn More Search the audit log for user and admin activity in Office 365 Search-UnifiedAuditLog Search the audit log in the Office 365 Security & Compliance Center Office 365 Management Activity API


New item
Exit grid view
All Items*
Filter (3)
Title
ore updated
Source
Categories
Solutions
Action Type
Document security assurance requirements in acquisition contracts
Compliance Score
Manage compliance
Compliance Manager
Documentation
Document the Information System Environment in the Acquisition Contract
Establish voip usage restrictions
Develop access control policies and procedures
Develop spillage response procedures
Discover and respond
Data investigation
Document Protection of Security-related Information in Acquisition Contracts
Review access control policies and procedures
Define and establish security and privacy attributes
Develop security safeguards
Document third-party security requirements
Develop Incident Response Plan - High Level Approach
Identify incident response personnel
Compliance Manager > Improvement actions > Develop Incident Response Plan - High Level Approach
Develop Incident Response Plan - High Level Approach
Overview
Implementation Status
Not Implemented
Test Status
None
Points achieved
0/9
Group
Default Group
Documents
0
Assigned to
None
Assign action
Implementation
Testing
Standards and Regulations
Documents
Implementation status
Select Implementation status...
Implementation date
Select a date...
How to implement
Your organization should develop an incident response plan that provides a high-level approach for how the incident response capability fits into the overall organization. Microsoft recommends that your organization create and maintain incident response policies and procedures to create an overall security incident response plan that describes the structure and organization of the incident response capability. Microsoft also recommends that you document and classify incidents into different categories for tracking purposes (for example, false positive, security incident, potential security breach, and incident with privacy impact). It is also recommended that your policies provide guidance for addressing each category of incidents defined by your organization as well as a high-level approach for how the incident response capability fits into the overall organization. Your organization should establish and implement a process for employeess, contractors, and third-party users to report any security incidents through appropriate communication channels.
Assigned to
None
Assign action
log data and look for any signs
activity.
Prerequisites and licensing requirements Before you begin searching the audit log
Launch Now
Learn More Search the audit log for user and admin activity in Office 365 Search-UnifiedAuditLog Search the audit log in the Office 365 Security & Compliance Center Office 365 Management Activity API


All Items*
Filter (3)
Categories
Solutions
Action Type
Manage compliance
Compliance Manager
Documentation
Discover and respond
Data investigation
CloudWay
Microsoft 365 compliance
Compliance Manager
Improvement actions
Develop Incident Response Plan - High Level Approach
Develop Incident Response Plan - High Level Approach
Overview
Implementation Status
Not Implemented
Test Status
None
Points achieved
0/9
Group
Default Group
Documents
0
Assigned to
None
Assign action
Implementation
Testing
Standards and Regulations
Documents
Implementation status
Select Implementation status...
Implementation date
Select a date...
How to implement
Your organization should develop an incident response plan that provides a high-level approach for how the incident response capability fits into the overall organization. Microsoft recommends that your organization create and maintain incident response policies and procedures to create an overall security incident response plan that describes the structure and organization of the incident response capability. Microsoft also recommends that you document and classify incidents into different categories for tracking purposes (for example, false positive, security incident, potential security breach, and incident with privacy impact). It is also recommended that your policies provide guidance for addressing each category of incidents defined by your organization as well as a high-level approach for how the incident response capability fits into the overall organization. Your organization should establish and implement a process for employeess, contractors, and third-party users to report any security incidents through appropriate communication channels.

NORDIC
– VIRTUAL SUMMIT –

5 Use Power Automate

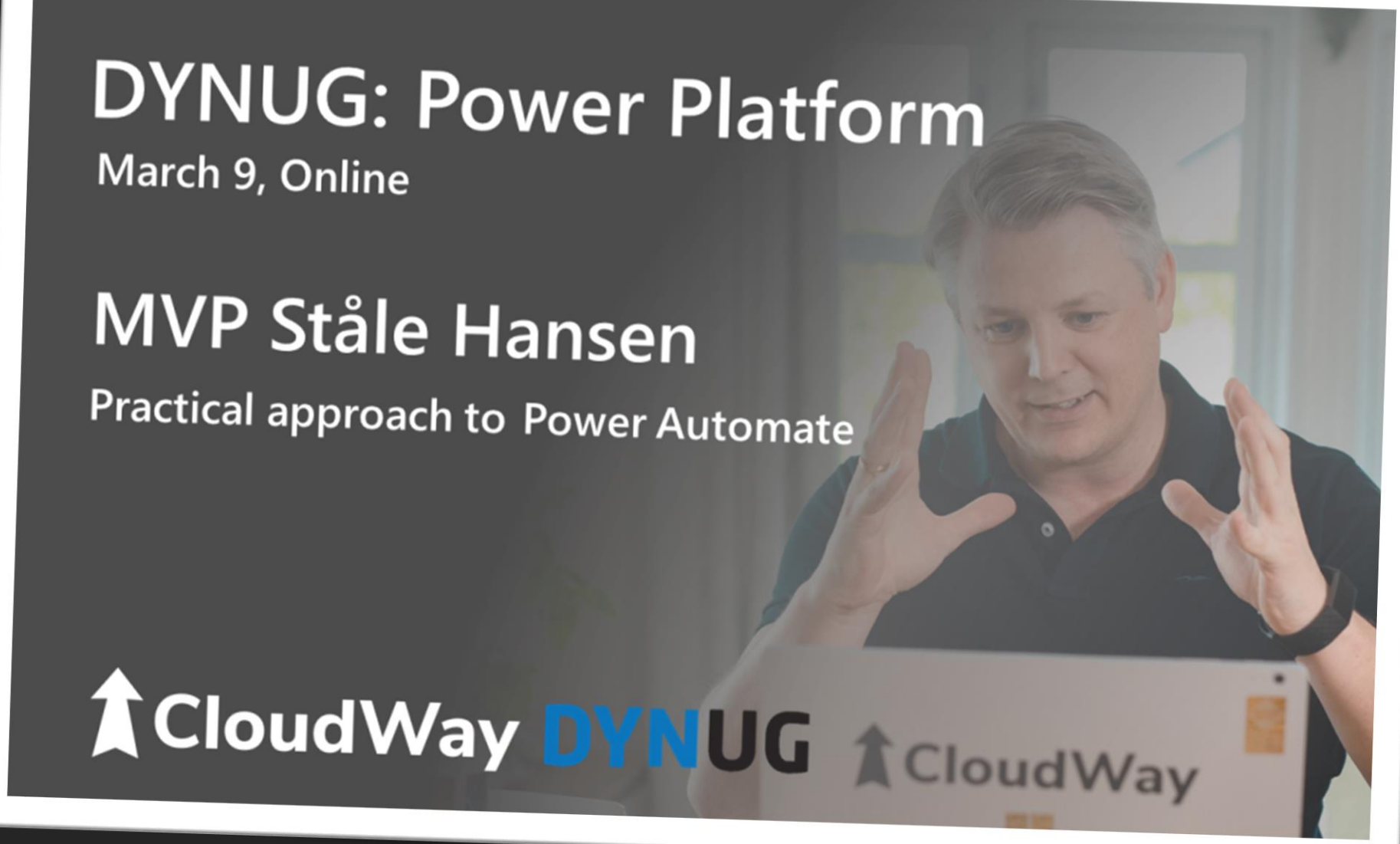
Use the SharePoint list trigger and create a planner task

DYNUG: Power Platform

March 9, Online

MVP Ståle Hansen

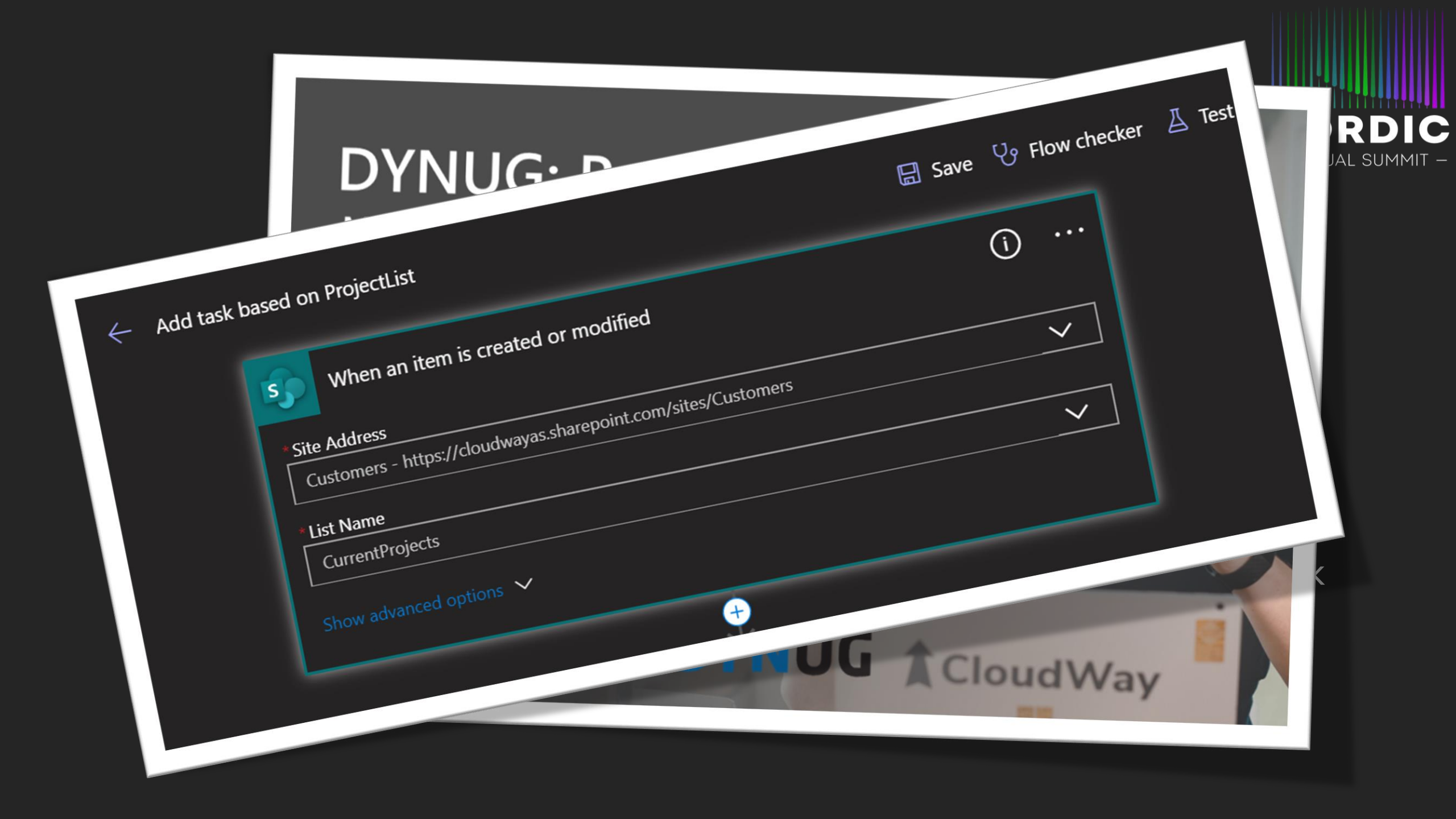
Practical approach to Power Automate



CloudWay DYNUG

RDIC

UAL SUMMIT –


DYNUG
Save
Flow checker
Test
Add task based on ProjectList
When an item is created or modified
* Site Address
Customers - https://cloudwayas.sharepoint.com/sites/Customers
* List Name
CurrentProjects
Show advanced options
CloudWay

NORDIC
– VIRTUAL SUMMIT –

6 Bonus

CSV compare find added actions over time

```powershell
#Importing the old compliance score csv's
$ComplianceScoreImport = Import-Csv -Path $Folder$ComplianceScore

#Importing the new compliance score csv's
$NewComplianceScoreImport = Import-Csv -Path $Folder$NewComplianceScore

$FinalAddedActions = @()
$addedCompleteScore = @()

if ($ComplianceScoreImport.count -lt $NewComplianceScoreImport.count){

    $compared = Compare-Object -ReferenceObject $ComplianceScoreImport.'Improvement action' -DifferenceObject $NewComplianceScoreImport.'Improvement action' | Where-Object {$_.SideIndicator -match "=>"}
    $count = $compared.count; $count--
    $FinalAddedActions = @()
    while ($count -ge 0){
        $AddedActions = $NewComplianceScoreImport | Where-Object {$_.'Improvement action' -match $compared.InputObject[$Count]}
        $count--
        $FinalAddedActions += $AddedActions
    }

    Write-host Number of new actions: @($FinalAddedActions).count

    #creating the extended compliance score list
    foreach ($Line in $FinalAddedActions){
                $addObject = Add-ExtendedAttributeList
                $addObject.ImprovementAction = $Line.'Improvement action'
                $addObject.Source = "Compliance Score"
                $addObject.Solutions = $Line.Solutions
                $addObject.Categories = $Line.Categories
                $addObject.PointsAchieved = $Line.'Points achieved'
                $addObject.ActionType = $Line.'Action Type'
                $addObject.Group = $Line.Group
                $addObject.Assessments = $Line.Assessments
                $addObject.DateImported = (Get-Date -Format "yyyy-MM-dd")
                $addedCompleteScore += $addObject

        }
        $addedCompleteScore.count
}
else{Write-host No new actions detected}
```

NORDIC
— VIRTUAL SUMMIT —


https://github.com/StaleHansen/Public

NORDIC
– VIRTUAL SUMMIT –

Result: confidence

This is how you drive security and compliance process in Microsoft 365!

#NVSummit2021

This is how you drive security and compliance process in Microsoft 365!

Ståle Hansen
Principal Cloud Architect @ CloudWay
@StaleHansen
Microsoft MVP & RD

Thanks for attending

NORDIC — VIRTUAL SUMMIT —

Please evaluate our session

NORDIC
– VIRTUAL SUMMIT –

Thank you!

System Center User Group
Finland
#SCUGFI

MSEndPointMgr.com
#MSEndPointMgr

Modern Management User Group
Norway
#MMUGNO

System Center User Group
Denmark

#SCUGDK

System Center User Group
Sweden
#SCUGSE

https://2021.nordicvirtualsummit.com/feedback