

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



Ståle Hansen

Principal Cloud Architect @ CloudWay

@StaleHansen

Microsoft MVP & RD

#NVSummit2021

This is how you drive security
in the compliance process in

CloudWay



<https://youtube.com/StaleHansen>

NORDIC

– VIRTUAL SUMMIT –

#NVSummit2021

This is how you drive security
in

CloudWay



<https://youtube.com/StaleHansen>

NORDIC

– VIRTUAL SUMMIT –



+ 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... ...nployees	Ståle Hansen	1	Low	Data Protection Baseline	Default Group	Azure Active Directory
Enforce Multi-Factor Authenticator Registratio... ...n	Ståle Hansen	1	Low	Data Protection Baseline	Default Group	Azure Active Directory
Set up ATP Safe Links policies				Data Protection Baseline	Default Group	Office 365 / Threat Protection
Enforce logical access				Data Protection Baseline	Default Group	Microsoft 365 center
Enable Policy to Block Legacy Authentication	Ståle Hansen	1	Low	Data Protection Baseline	Default Group	Azure Active Directory
Use boundary protection devices for unclas... ...ified data				Data Protection Baseline	Default Group	Compliance Manager



+ New item

Edit in grid view

...

Title

Assigned to

Priority

Amount of work

Regulations

Group

Solutions

Auto-...

Ståle Hansen

2

High

Data Protection
Baseline

Default Group

Information
protection

My Buddy

Ståle Hansen

1

Low

Data protection
Baseline

Default Group

Compliance
Manager

Ståle Hansen

Ståle Hansen

1

Low

Data protection
Baseline

Default Group

Azure Active
Directory

Ståle Hansen

Ståle Hansen

2

High

Data Protection
Baseline

Default Group

Azure Active
Directory

Lists

Enable Policy to Block Legacy Authentication

Ståle Hansen

1

Low

Data Protection
Baseline

Default Group

Azure Active
Directory

Use boundary protection devices for unclas...

Data Protection
Baseline

Default Group

Compliance
Manager

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



+ New item

Edit in grid view

← Add task based on ProjectList

Save

Flow checker

Test



Lists

Enforce logical access

Enable Policy to Block Legacy Authentication

Ståle Hansen

1

Low

Data Protection
Baseline

Default Group

Azure Active
Directory

Use boundary protection devices for unclas...

Data Protection
Baseline

Default Group

Compliance
Manager

When an item is created or modified



...

* Site Address

Customers - https://cloudwayas.sharepoint.com/sites/Customers



* List Name

CurrentProjects



Show advanced options



Baseline



Consultant



Microsoft 365

Consultant



Customer



Microsoft 365



Customer



2020
Microsoft 365



Customer

2021
Microsoft 365



Customer

2022
Microsoft 365



Customer

2023

Microsoft 365



225 Message Center since April 2020

Major updates: 71

User Impacts: 126

New Features: 79

2 Drivers for sustainability

1

Someone must own the tenant roadmap

This is preferably the customer



M365 and Azure AD Admin Tools

Controls for Groups,
Identity, Licenses, Access



Office 365 Admin Tools

Controls for managing Exchange,
SharePoint and Teams
features



Security & Compliance Admin Tools

Controls for managing
Security & Compliance
across M365



M365 and Azure AD
Admin Tools

Controls for Groups,
Identity, Licenses, Access



Office 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?

2

Use Secure Score and Compliance Score

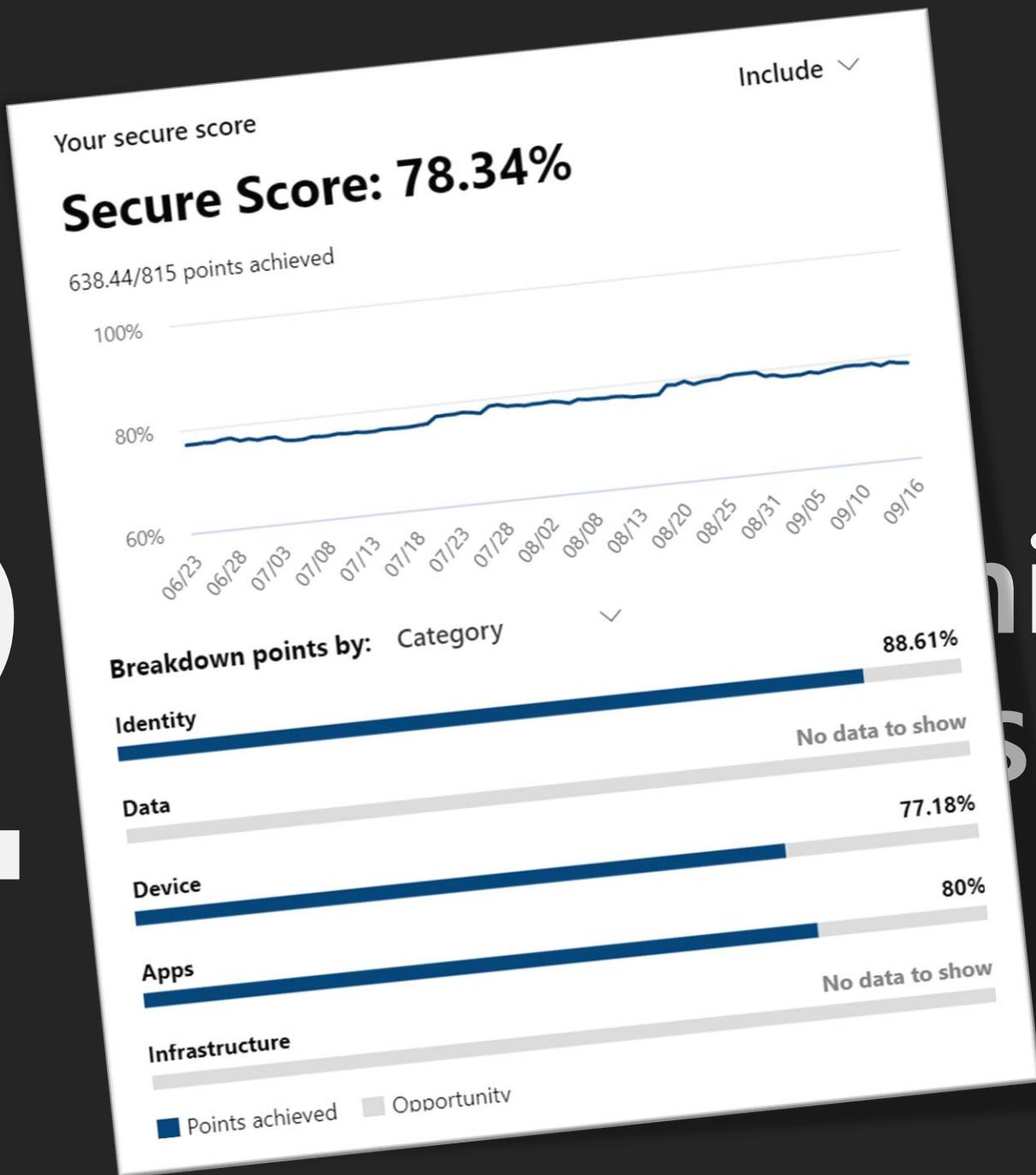
406 actions for a secure and compliance tenant

2

You need admin rights to access the scores

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

2



min 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.

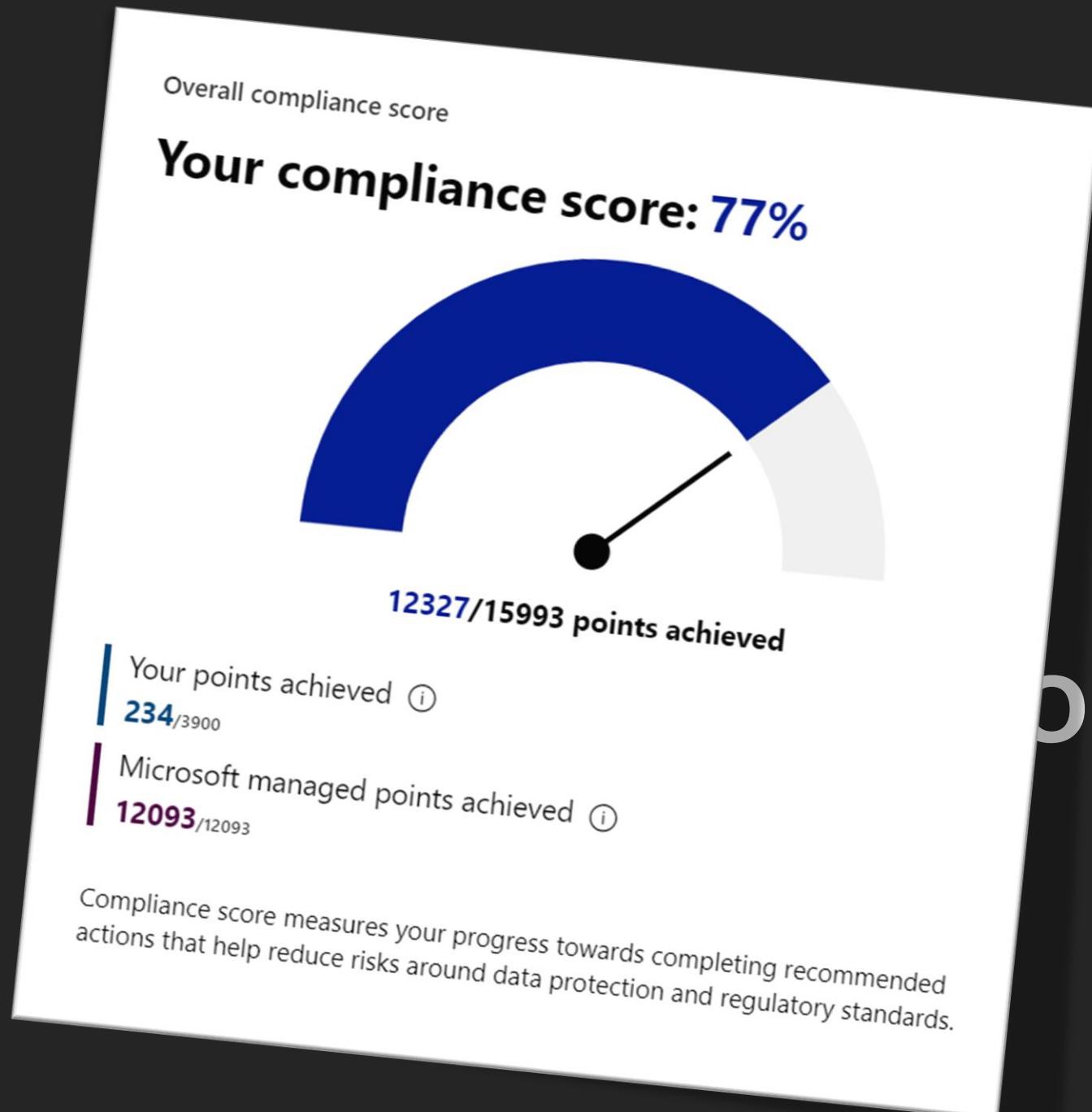
↓ Export

Applied filters:

Rank	Improvement action	Score impact	Points achieved	Status
128	Disable 'Domain member: Disable machine account password changes'	+0.23%	2/2	Completed No Regressed
129	Turn on customer lockbox feature	+0.11%	1/1	Completed No
130	Discover trends in shadow IT application usage	+0.11%	1/1	Completed No
131	Designate more than one global admin	+0.11%	1/1	Alternate mitigation 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 honeypot 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

2



rights
ores

2

Overall

Compliance Manager

Overview Improvement actions Solutions Assessments Assessment templates

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

Filter

Regulations: Any Solutions: Any Groups: Any Test Status: Any Categories: Any Assigned To: Any

280 items Search

Export Accept all updates Assign to user

Improvement action	Points achi...	Regulations	Group	Solutions	Assessments
Enable audit log search	0/27	Data Protection Baseline	Default Gro...	Audit	Data Protection Baseline
Auto-Apply Sensitivity Labels	0/27	Data Protection Baseline	Default Gro...	Information pr...	Data Protection Baseline
Require mobile devices to block ...	0/27	Data Protection Baseline	Default Gro...	Intune	Data Protection Baseline
Create a device configuration pr...	27/27	Data Protection Baseline	Default Gro...	Intune	Data Protection Baseline
Enable multi-factor authenticatio...	27/27	Data Protection Baseline	Default Gro...	Azure Active Di...	Data Protection Baseline
Enforce multi-factor authenticat...	27/27	Data Protection Baseline	Default Gro...	Azure Active Di...	Data Protection Baseline
Set up ATP safe links policies	0/27	Data Protection Baseline	Default Gro...	Microsoft Defe...	Data Protection Baseline
Enable policy to block legacy aut...	27/27	Data Protection Baseline	Default Gro...	Azure Active Di...	Data Protection Baseline

ghts
S

5 Steps

Creating the list

1

Download the CSV's

Import to excel and add custom columns

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

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 threats
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

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		

- 1 Apply sensitivity labels to protect sensitive data
- 2 Activate Azure Rights Management
- 3 Require Mobile Devices to Use Encryption
- 4 Create a compliance policy for Android enterprise devices
- 5 Enforce rules of behavior and access agreements
- 6 Create a device configuration profile for Android enterprise devices
- 7 Implement Replay Resistant Authentication Mechanisms - Privileged Accounts

Compliance Score	Default Group	Compliance Manager	Data Protection Baseline
Compliance Score	Default Group	Compliance Manager	Data Protection Baseline
Compliance Score	Default Group	Intune	Data Protection Baseline
Compliance Score	Default Group	Azure Active Directory	Data Protection Baseline

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 threats
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

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	

- 1 Apply sensitivity labels to protect sensitive data
- 2 Activate Azure Rights Management
- 3 Require Mobile Devices to Use Encryption
- 4 Create a compliance policy for Android enterprise devices
- 5 Enforce rules of behavior and access agreements
- 6 Create a device configuration profile for Android enterprise devices
- 7 Implement Replay Resistant Authentication Mechanisms - Privileged Accounts

Source	Group	Compliance Manager
Compliance Score	Default Group	Compliance Manager
Compliance Score	Default Group	Intune
Compliance Score	Default Group	Azure Active Directory
Compliance Score	Default Group	Compliance Manager

Source	Group	Compliance Manager
Compliance Score	Default Group	Control access

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 threats
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

	Implementation Status	Test status	Tested date	Score updated	Source
Not implemented, needs validation	Not Planned	None			Compliance Score
Not implemented, needs validation	Implemented	Not Tested		No	Compliance Score
		Could not be detected		No	Compliance Score
		Could not be detected			Compliance Score
		None			Compliance Score
1. Apply sensitivity labels to protect sensitive data	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	Compliance Score
2. Activate Azure Rights Management	Compliance Score	Default Group	Compliance Manager	Data Protection Baseline	Control access
3. Require Mobile Devices to Use Encryption	Compliance Score	Default Group	Intune	Data Protection Baseline	Control access
4. Create a compliance policy for Android enterprise devices	Compliance Score	Default Group	Azure Active Directory	Data Protection Baseline	Control access
5. Enforce rules of behavior and access agreements	Compliance Score				
6. Create a device configuration profile for Android enterprise devices	Compliance Score				
7. Implement Replay Resistant Authentication Mechanisms - Privileged Accounts	Compliance Score				

E	F
Assessments	Categories
Protection Baseline	Protect information
Data Protection Baseline	Control access
Data Protection Baseline	Control access
Data Protection Baseline	Control access
Data Protection Baseline	Protect against threats
Data Protection Baseline	Control access
Data Protection Baseline	Manage compliance
Data Protection Baseline	Protect information
Data Protection Baseline	Manage compliance
Data Protection Baseline	Manage compliance
Data Protection Baseline	Manage compliance
Data Protection Baseline	Manage devices
Data Protection Baseline	Manage devices
Data Protection Baseline	Control access

updated	Source
	Compliance Score

Data Protection --
Data Protection Baseline Control access

```

5 ## Script to merge compliance score and secure score and adding custom attributes
6 ######
7 ######
8 ######
9 ######
10 ######
11 ######
12 ######
13 ######
14 ######
15 ######
16 ######
17 ######
18 ######
19 ######
20 ######
21 ######
22 ######
23 function Add-ExtendedAttributeList{
24     New-Object -TypeName PSCustomObject -Property @{
25         ImprovementAction = $null
26         Priority = $null
27         Effort = $null
28         Responsible = $null
29         TechnicalResource = $null
30         Comment = $null
31         ImplementationStatus = $null
32         TestStatus = $null
33         TestedDate = $null
34         ScoreUpdated = $null
35         Source = $null
36         Solutions = $null
37         Categories = $null
38         PointsAchieved = $null
39         ActionType = $null
40         Regulations = $null
41         Group = $null
42         Assessments = $null
43         DateImported = $null
44         LastSynced = $null
45         MicrosoftUpdate = $null
46         ScoreImpact = $null
47         Regressed = $null
48         HaveLicense = $null
49         Description = $null
50         Documentation = $null
51     }
52 }
53

```

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-national security information	
Manage Calendar Details Sharing	
Limit Consecutive Logon Failures	

Implementation Status

Requires resources and needs	Not Planned
Implemented, needs validation	Implemented

B

1 Anonymize sensitive data	
1 Apply sensitivity labels to protect sensitive data	
2 Activate Azure Rights Management	
3 Require Mobile Devices to Use Encryption	
4 Create a compliance policy for Android enterprise devices	
5 Enforce rules of behavior and access agreements for mobile devices	
6 Create a device configuration profile for Android devices	
7 Implement Replay Resistant Authentication	

E	F
nts	Categories
ction Baseline	Protect information
ction Baseline	Control access
ction Baseline	Control access
ction Baseline	Protect against threa
ction Baseline	Control access
ction Baseline	Manage compliance
ction Baseline	Protect information
ction Baseline	Manage compliance
ction Baseline	Manage compliance
ction Baseline	Manage compliance
ction Baseline	Manage devices
ction Baseline	Manage devices
ction Baseline	Control access
ction Baseline	

E	F
nses and needs	Source
Not Planned	Compliance Score
Planned, needs va	Compliance Score
nted, needs va	Compliance Score
nted, needs va	Compliance Score
nted, needs va	Compliance Score
nted, needs va	Compliance Score

ction Baseline Control access

```

5      ## Script to m...
6
7      ## Script to m...
8
9
10
11
12
13
14
15

#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

```

Implementation actions	Planned, needs validation
Auto-Apply Sensitivity Labels	Not Planned
Enable Multi-factor Authentication	Planned, needs validation
Enforce Multi-Factor Authentication	Planned, needs validation
Set up ATP Safe Links policies	Planned, needs validation
Enforce logical access	Planned, needs validation
Use boundary protection devices	Planned, needs validation
Manage Calendar Details Sharing	Planned, needs validation
Limit Consecutive Logon Failures	Planned, needs validation

- Anonymity
- 1 Apply sensitivity labels to protect
- 2 Activate Azure Rights Management
- 3 Require Mobile Devices to Use En
- 4 Create a compliance policy for An
- 5 Enforce rules of behavior and acc
- 6 Create a device configuration pro
- 7 Implement Replay Resistant Auth

Implementation

nses and needs Not Planned
nted, needs va Implemented



E	F
ts	Categories
ction Baseline	Protect information
ction Baseline	Control access
ction Baseline	Control access
ction Baseline	Protect against threa
ction Baseline	Control access
ction Baseline	Manage compliance
ction Baseline	Protect information
ction Baseline	Manage compliance
ction Baseline	Manage compliance
ction Baseline	Manage devices
ction Baseline	Manage devices
ction Baseline	Control access
ction Baseline	

▼ Source

Compliance Score
Compliance Score
Compliance Score
Compliance Score
Compliance Score

PS C:\Temp>

Comment, Regulations, Group, HaveLicense, Documentation



<https://github.com/StaleHansen/Public>

```
2 #By Ståle Hansen, Twitter: @StaleHansen
3 #####
4 ## Script to merge compliant
5 #####
6 #####
7 #####
```

2

Adjust Secure Score CSV

And import into the same document as compliance score

396	Create a custom activity policy to discover suspicious usage patterns				
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 Azure AD
404	Set a honeypot 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					
408					

, and import into the same document as compliance score

V



– VIRTUAL SUMMIT –

395	Create a custom activity policy to disc
397	Disable 'Domain member: Disable ma
398	Turn on customer lockbox feature
399	Discover trends in shadow IT applicat
400	Designate more than one global adm
401	Use limited administrative roles
402	Remove TLS 1.0/1.1 and 3DES depen
403	Fix Advanced Audit Policy issues
404	Set a honeypoint account
405	Configure VPN integration
406	Configure Microsoft Defender for E
407	
408	

```

2 #By Ståle Hansen, Twitter: @StaleHansen
3
4 ##### Script to merge compliance score and secure score and adding custom attributes
5
6 ##### Script to merge compliance score and secure score and adding custom attributes
7
8 $Folder = "C:\Temp\"
9 $ComplianceScore = "Compliance Manager - Microsoft 365 compliance.csv"
10 $SecureScore = "Microsoft Secure Score - Microsoft 365 security.csv"
11 $NewComplianceScore = "New Compliance Manager - Microsoft 365 compliance.csv"
12 $NewSecureScore = "New Microsoft Secure Score - Microsoft 365 security.csv"
13
14
15
16
17
18
19 #####
20 ## Create an object that has all the attributes we want
21 #####
22
23 function Add-ExtendedAttributeList{...}
24
25 #####
26 ## Import the scores and create the complete score list
27 #####
28
29 #Importing the score csv's
30 $ComplianceScoreImport = Import-Csv -Path $Folder\$ComplianceScore
31 $SecureScoreImport = Import-Csv -Path $Folder\$SecureScore
32
33 $CompleteScore = @()
34
35 #creating the extended compliance score list
36 foreach ($Line in $ComplianceScoreImport){...}
37
38 #creating the extended secure score list
39 foreach ($Line in $SecureScoreImport){...}
40
41 $CompleteScore.ImprovementAction
42 $CompleteScore.Count|_
43 Select-Object -Property ImprovementAction, Priority, Effort, Responsible, TechnicalResource,
44 Comment, ImplementationStatus, TestStatus, TestedDate, Scoreupdated, Source, Solutions, Categories, ActionType,
45 Regulations, Group, Assessments, DateImported, PointsAchieved, LastSynced, MicrosoftUpdate, ScoreImpact, Regressed,
46 HaveLicense, Documentation, Description | Export-Csv -Path $Folder"CompleteScore.csv" -NoTypeInformation -Encoding UTF8
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116

```

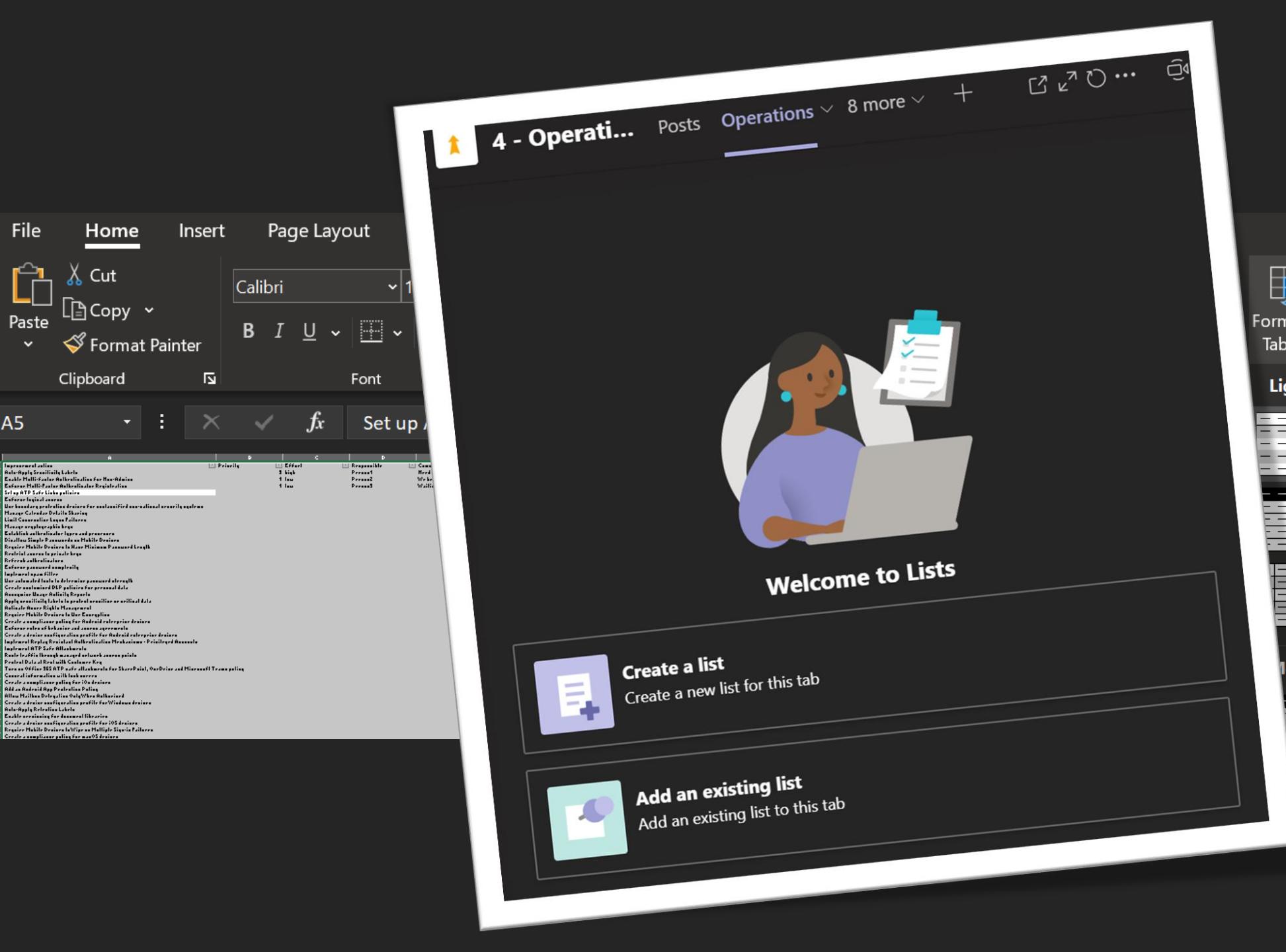
3

Format as table

And import into Microsoft Lists



The screenshot shows the Microsoft Excel ribbon with the 'Home' tab selected. The ribbon tabs are: File, Home, Insert, Page Layout, Formulas, Data, Review, View, Help. Under the Home tab, there are sections for Clipboard, Font, Alignment, Number, and Conditional Formatting. The Conditional Formatting section has a 'Format as Table' dropdown and a preview of 'White, Table Style Light 1'. The main area shows a table with the title 'Set up ATP Safe Links policies'.



The screenshot shows the Microsoft Lists interface. At the top, there's a navigation bar with tabs like 'Posts' and 'Operations'. Below the navigation bar, there's a large central area featuring a woman working on a laptop with a clipboard icon above her. The text 'Welcome to Lists' is displayed below her. On the left side, there's a ribbon menu with 'Home' selected, and a table view showing various policy items. On the right side, there's a 'Format as Table' section with a preview and a grid of table styles.

File Home Insert Page Layout

Cut Copy Format Painter

Clipboard

Font

A5

Calibri 11

B I U

Priority Effect

Responsible Person

Created By

Last Modified By

Created Date

Last Modified Date

Comments

Attachments

File

Operations 8 more +

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

The screenshot shows a Microsoft SharePoint document library interface. At the top, there's a navigation bar with a yellow arrow icon, the title "4 - Operati...", "Posts", "Operations", "8 more", a plus sign, and various sharing and settings icons. On the left, a ribbon menu is open with "Home" selected, showing options like Paste, Cut, Copy, Format Painter, and Clipboard. Below the ribbon, the text "From Excel" is displayed, followed by the instruction "Select an Excel file from your device or this site." Two buttons are present: "Upload from this device" and "Upload file". Further down, the text "Choose a file already on this site" is shown, followed by a section titled "Documents". This section lists files with columns for Name and Modified. The visible file names include:

- Imported.xlsx
- InfoPath Form Library
- Excel Multi-factor authentication for Non-RM users
- Excel Multi-factor authentication Registrations
- Setup ATP Safe Links policies
- Enforce logical access
- Configure mobile devices for identified non-compliant systems
- Mobile Device Details Sharing
- Limit Conversation Length Policies
- Mobile Device Protection
- Mobile Device Protection and enforcement
- Require Single Passcode on Mobile Devices
- Require Mobile Devices to Meet Minimum Password Length
- Require a strong password length
- Enforce account complexity
- Implement spam filters
- Configure mobile devices for alternative password strength
- Configure mobile DLP policies for personal data
- Responsible Usage Mobile Reports
- Replace sensitive labels in personal documents or critical data
- Configure mobile DLP policies for personal data
- Require Mobile Devices to Use Encryption
- Create a compliance policy for Android enterprise devices
- Configure mobile devices for mobile app management
- Configure mobile devices for mobile device management
- Implement Biometric Authentication Mechanisms - Privacy and Residual
- Implement SFTP Safe Browsing
- Protect Office 365 SFTP safe storage for SharePoint, OneDrive and Microsoft Teams policy
- Configure a compliance policy for the devices
- Add an Android App Protection Policy
- Allow Multiple Downloads Only/One Rekey/Reprotect
- Create a device configuration profile for Windows devices
- Enable enrollment for domain-joined devices
- Create a device configuration profile for iOS devices
- Require Mobile Devices to Use on Multiple Sieve Policies
- Create a compliance policy for macOS devices

4 - Operati...

Posts

Operati...

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 Priority Choice Effort Do not import Responsible

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-national security systems

Manage Calendar Details

Sharing

Limit Consecutive Logon Failures

Person1

Person2

Person3

Single line of text

Comment

Need evaluate E5 licenses and needs

We believe its implemented, needs validation

Waiting feedback

Choice

Implementation Status

Not Planned

Implemented

Waiting feedback

Choice

Test status

None

Not Tested

Could not be detected

Could not be detected

None

None</p

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 Registrat... 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 selected

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	

File

Paste

A5

Imported tables

- 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-national security systems
- Manage Calendar Details Sharing
- Limit Consecutive Logon Failures

Good

Input

Color palette:

- Choice
- Test status
- None
- Not Tested
- Could not be detected
- None
- None
- None
- None
- None

The image is a collage of several screenshots from Microsoft Excel, illustrating various features and configurations:

- Top Left:** A screenshot of the "Customize" dialog box. It shows a preview of a table with columns for "Title", "Priority", and "Improvement action". Below the preview, there's a list of items such as "Auto-Apply Sensitivity Labels", "Enable Multi-factor Authentication for Non-Admins", and "Enforce Multi-Factor Authenticator Registration".
- Top Center:** A screenshot of a table with columns: "Comment", "Implementation Sta...", "Test status", and "Tested date". The "Test status" column has dropdown options: "None", "Not Tested", and "Not be...". The "Column settings" menu is open, showing options like "Edit", "Format this column", "Move left", "Move right", "Hide this column", "Pin to filters pane", "Show/hide columns", and "Add a column".
- Bottom Left:** A screenshot of the "Column settings" menu, specifically the "Add a column" section. It lists several data types: "None", "Yes/No", "Person", "Date and time", and "Choice".
- Bottom Right:** A screenshot of a table with columns: "Comment", "Implementation Sta...", "Test status", and "Tested date". The "Test status" column has dropdown options: "None", "Not Tested", "Could not be detected", and "None".

Lists

[+ New item](#)[Edit](#)[Edit in grid view](#)[Copy link](#)[Delete](#)[...](#)[Title](#)[Priority](#)[Effort](#)[Responsible](#)[Comment](#)[Implementation Sta...](#)[Test status](#)[Tested date](#)[Auto-Apply Sensitivity Labels](#)

3

high

My Buddy

Need evaluate E5
licenses and needs

Not Planned

None

[Score updated](#)[Source](#)[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 Registr...](#)

1

low

My Buddy

Waiting feedback

Test failed

[No](#)[Compliance Score](#)[Set up ATP Safe Links policies](#)

My Buddy

None

[Yes](#)[Compliance Score](#)[Enforce logical access](#)

My Buddy

None

[No](#)[Compliance Score](#)[Use boundary protection devices for unclas...](#)

My Buddy

None

[Yes](#)[Compliance Score](#)[Manage Calendar Details Sharing](#)

My Buddy

None

[Yes](#)[Compliance Score](#)[Enforce logical ac...](#)

Use boundary protection
devices for unclassified non-
national security systems

Manage Calendar Details
Sharing

Limit Consecutive Logon
Failures

None

Date and time

None

Choice

[Save](#)[Delete](#)

4 Delegate and document

The hard work

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

Implementation Status	Test Status
Could not be detected	Could not be detected

Points achieved: 0/27

Documents: 0

Assigned to: None

Implementation status: Select Implementation status...

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

All Items*

Comment

Need evaluate E5 licenses and needs

We believe its implemented, needs validation

Waiting feedback

CloudWay Microsoft 365 compliance

https://compliance.microsoft.com/compliancemanager?viewid=ImprovementActions

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](#)

Implementation status: Could not be detected

Overview

Implementation Status	Test Status
Could not be detected	Could not be detected
Points achieved	Group
0/27	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 minimum level of security enabled in all editions of Azure AD.

https://compliance.microsoft.com/compliancemanager?viewid=Improvem...

Office 365 compliance

+ New item | Exit grid view ...

Title: Turn on Microsoft Defender for Endpoint sensor

Source: Secure Score

Categories: Defender for Endpoint

Action Type: Technical

Assessments: Device

Title: Ensure BitLocker drive compatibility

Source: Secure Score

Categories: Defender for Endpoint

Action Type: Technical

Assessments: Device

Title: Restrict anonymous users from joining meetings

Source: Secure Score

Categories: Microsoft Teams

Action Type: Technical

Assessments: Apps

Title: Enable self-service password reset

Source: Secure Score

Categories: Azure Active Directory

Action Type: Technical

Assessments: Identity

Title: Turn on sign-in risk policy

Source: Secure Score

Categories: Azure Active Directory

Action Type: Technical

Assessments: Identity

Title: Turn on user risk policy

Source: Secure Score

Categories: Azure Active Directory

Action Type: Technical

Assessments: Identity

Title: Enable policy to block legacy authentication

Source: Secure Score

Categories: Azure Active Directory

Action Type: Technical

Assessments: Identity

Title: Enable Microsoft Defender Antivirus scanning of downloaded files and attachments

Source: Secure Score

Categories: Defender for Endpoint

Action Type: Technical

Assessments: Device

Title: Turn on Microsoft Defender Firewall

Source: Secure Score

Categories: Defender for Endpoint

Action Type: Technical

Assessments: Device

Title: Turn on real-time protection

Source: Secure Score

Categories: Defender for Endpoint

Action Type: Technical

Assessments: Device

Title: Turn on Microsoft Defender Antivirus

Source: Secure Score

Categories: Defender for Endpoint

Action Type: Technical

Assessments: Device

Title: Enable Microsoft Defender Antivirus email scanning

Source: Secure Score

Categories: Defender for Endpoint

Action Type: Technical

Assessments: Device

Title: Block Adobe Reader from creating child processes

Source: Secure Score

Categories: Defender for Endpoint

Action Type: Technical

Assessments: Device

0/21 Documents 0 Assigned to None

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 Last updated: 5 days ago

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

Implementation

Prerequisites

- ✓ You have Azure Active Directory Premium

Next steps

In Azure AD Identity Protection you can configure user risk remediation policy. For the users you need to set the conditions (risk level) in which the policy triggers and whether access is blocked when the policy is triggered. Switch the state of ON.

Implementation status

You have 5 users out of 60 that do not have MFA enabled.

Learn more

None

and data that are used for 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 minimum level of security enabled in all editions of Azure AD.

https://app.cloudway.com/improvementmanager?viewid=Improvement...  CloudWay Microsoft 365 security

All Items* Filter (1)

Action Type	Assessments
Technical	Device
Technical	Device
Technical	Apps
Technical	Identity
Technical	Device

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

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

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 Premium

Next steps
In [Azure AD Identity Protection](#) you can configure a user risk remediation policy. For the users in your organization, you need to set the conditions (risk level) under which the policy triggers and whether access is blocked when the policy is triggered. Switch the state of the policy to **ON**.

Implementation status
You have 5 users out of 60 that do not have the policy enabled.

Learn more
None

Improvement actions > Review audit data

CloudWay Microsoft 365 security

All Items* Filter (1)

Action Type Assessments

Technical Device

Technical Device

New item Exit grid view

Title

Use system clocks for audit records

Review alerts triggered by alert policies

Review audit data

Review File and Folder Activity

Add new item

Score updated

Source Categories Solutions Action Type

Compliance Score Discover and respond Audit Operational

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

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.

Resolved through third party

Resolved through alternate mitigation

Notes:

Write a note

Implementation status

You have 5 users out of 60 that do not have policy enabled.

Learn more

None

https://compliance.microsoft.com/compliance/audits/.../actions/.../improvementmanager?viewid=ImprovementManager

CloudWay Microsoft 365 security

All Items* Filter (1)

Action Type Assessments

Technical Device

All Items* Filter (4)

Solutions Action Type

Categories Discover and respond Audit Operational

Implementation Microsoft 365 compliance

CloudWay Microsoft 365 compliance

Compliance Manager > Improvement actions > Review audit data

Review audit data

Implementation Testing Standards and Regulations Documents

Implementation status Select Implementation status... Implementation date Select a date...

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

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

Compliance Score - Manage compliance				
Title	Created updated	Source	Categories	Solutions
Document security assurance requirements in acquisition contracts	Compliance Score	Manage compliance	Compliance Manager	Documentation
Document the Information System Environment in the Acquisition Contract	Compliance Score	Manage compliance	Compliance Manager	Documentation
Establish voip usage restrictions	Compliance Score	Manage compliance	Compliance Manager	Documentation
Develop access control policies and procedures	Compliance Score	Manage compliance	Compliance Manager	Documentation
Develop spillage response procedures	Compliance Score	Discover and respond	Data investigation	Documentation
Document Protection of Security-related Information in Acquisition Contracts	Compliance Score	Manage compliance	Compliance Manager	Documentation
Review access control policies and procedures	Compliance Score	Manage compliance	Compliance Manager	Documentation
Define and establish security and privacy attributes	Compliance Score	Manage compliance	Compliance Manager	Documentation
Develop security safeguards	Compliance Score	Manage compliance	Compliance Manager	Documentation
Document third-party security requirements	Compliance Score	Manage compliance	Compliance Manager	Documentation
Develop Incident Response Plan - High Level Approach	Compliance Score	Manage compliance	Compliance Manager	Documentation
Identify incident response personnel	Compliance Score	Manage compliance	Compliance Manager	Documentation

Compliance Manager > Improvement actions > Develop Incident Response Plan - High Level Approach

Develop Incident Response Plan - High Level Approach

Overview

Implementation Status	Test Status
Not Implemented	None
Points achieved	Group
0/9	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 employees, contractors, and third-party users to report any security incidents through appropriate communication channels.

All Items* Filter (3)

Categories Solutions Action Type

Score	Manage compliance	Compliance Manager	Documentation
Score	Manage compliance	Compliance Manager	Documentation
core	Manage compliance	Compliance Manager	Documentation
core	Manage compliance	Compliance Manager	Documentation
ore	Discover and respond	Data investigation	Documentation
ore	Manage compliance	Compliance Manager	Documentation
ore	Manage compliance	Compliance Manager	Documentation
re	Manage compliance	Compliance Manager	Documentation
re	Manage compliance	Compliance Manager	Documentation
e	Manage compliance	Compliance Manager	Documentation
e	Manage compliance	Compliance Manager	Documentation
e	Manage compliance	Compliance Manager	Documentation
e	Manage compliance	Compliance Manager	Documentation
	Manage compliance	Compliance Manager	Documentation

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	Test Status
Not Implemented	None

Points achieved 0/9

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 employees, contractors, and third-party users to report any security incidents through appropriate communication channels.

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

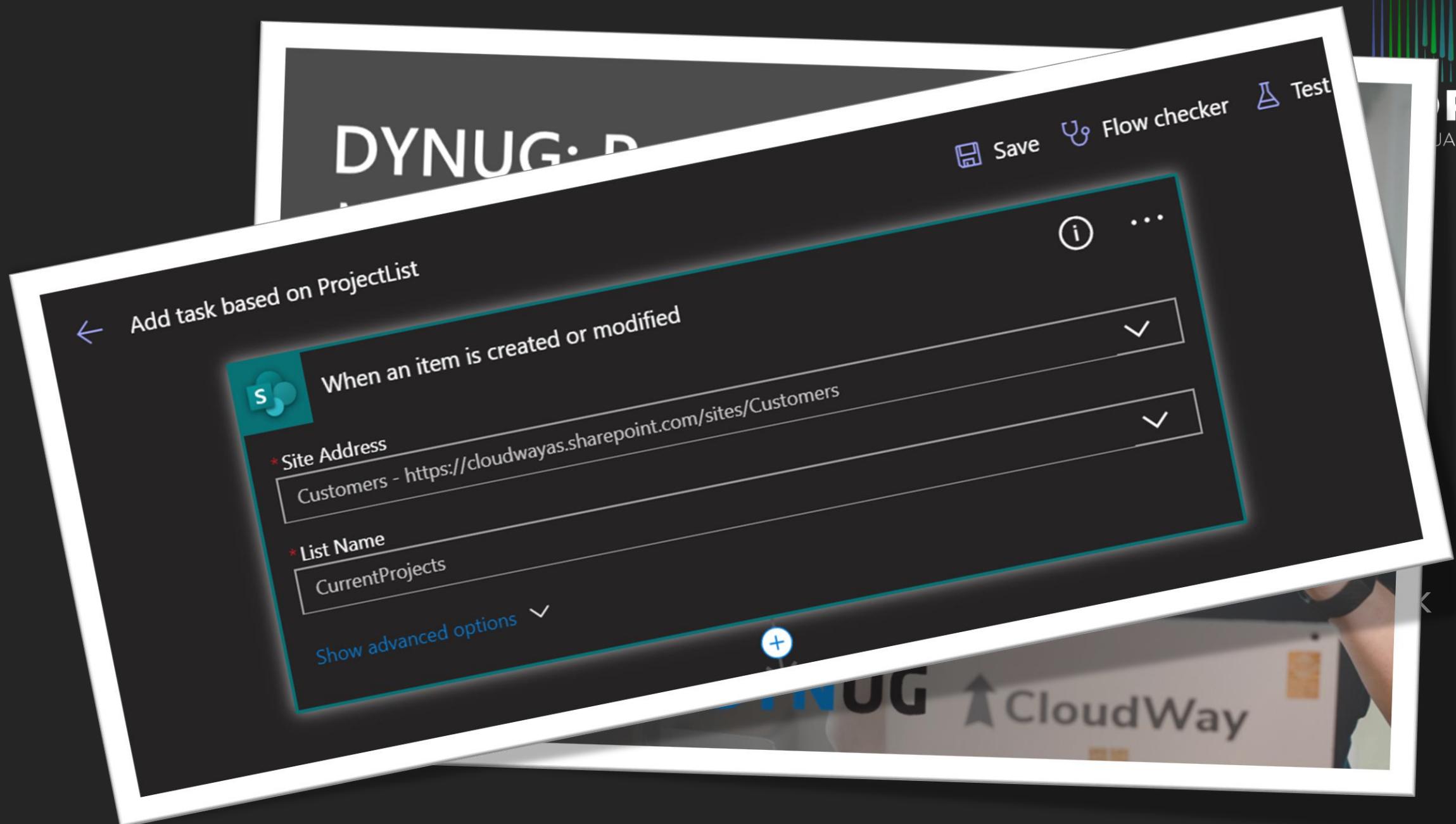


CloudWay **DYNUG**



CloudWay





6 Bonus

CSV compare find added actions over time

```
#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}
```

```

#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 -DifferenceObject $NewComplianceScoreImport
    $count = $compared.count; $count--
    $FinalAddedActions = @()
    while ($count -ge 0) {
        $AddedActions = $NewComplianceScoreImport | Select-Object -Property ImprovementAction, Priority, Responsible, TechnicalResource, Comment, ImplementationStatus, TestStatus, TestedDate, ScoreUpdated, Effort, Categories, ActionType, Regulations, Group, Assessments, DateImported, PointsAchieved, Source, Solutions, Documentation, HaveLicense, Description | Export-Csv -Path $Folder"AddedCompleteScore.csv" -NoTypeInformation -Encoding UTF8
        $addedCompleteScore += $AddedActions
        $count--
        $FinalAddedActions += $AddedActions
    }
    Write-host Number of new actions: @($FinalAddedActions)
    #creating the extended compliance score
    foreach ($Line in $FinalAddedActions) {
        $addObject = Add-ExtendedObject
        $addObject.ImprovementAction = $Line.ImprovementAction
        $addObject.Source = "Compliance"
        $addObject.Solutions = $Line.Solutions
        $addObject.Categories = $Line.Categories
        $addObject.PointsAchieved = $Line.PointsAchieved
        $addObject.ActionType = $Line.ActionType
        $addObject.Group = $Line.Group
        $addObject.Assessments = $Line.Assessments
        $addObject.DateImported = $Line.DateImported
        $addedCompleteScore += $addObject
    }
    $addedCompleteScore.count
} else{write-host No new actions detected}

```

```

143 ## Find new score actions
144 #####
145 $Folder = "C:\Temp\"
146 $ComplianceScoreImport = Import-Csv -Path $Folder$ComplianceScore
147 $NewComplianceScoreImport = Import-Csv -Path $Folder$NewComplianceScore
148 $FinalAddedActions = @()
149 $addedCompleteScore = @()
150
151 if ($ComplianceScoreImport.count -lt $NewComplianceScoreImport.count){...}
152 else{write-host No new actions detected}
153
154 #Importing the old secure score csv's
155 $SecureScoreImport = Import-Csv -Path $Folder$SecureScore
156 $NewSecureScoreImport = Import-Csv -Path $Folder$NewSecureScore
157
158 if ($SecureScoreImport.count -lt $NewSecureScoreImport.count){...}
159 else{write-host No new actions detected}
160
161 $addedCompleteScore.ImprovementAction = $NewSecureScoreImport | Select-Object -Property ImprovementAction, Priority, Responsible, TechnicalResource, Comment, ImplementationStatus, TestStatus, TestedDate, ScoreUpdated, Effort, Categories, ActionType, Regulations, Group, Assessments, DateImported, PointsAchieved, Source, Solutions, Documentation, HaveLicense, Description | Export-Csv -Path $Folder"AddedCompleteScore.csv" -NoTypeInformation -Encoding UTF8

```



<https://github.com/StaleHansen/Public>

```
ch "=>"}
```

```
119 ## Find new score actions
120 #####
121 $Folder = "C:\Temp\"  
122 #####
123 ##
```

```
#Imp  
$Comp  
  
#Impo  
$NewC  
  
$Fina  
$addee  
  
if ($C  
    $co  
    $co  
    $Fi  
    whi  
  
}  
  
writ  
  
#crea  
forea  
  
}  
}  
else{Write-H
```

Result: confidence

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



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

Please evaluate our session



Thank you!

MSEndPointMgr.com
#MSEndPointMgr

System Center User Group
Denmark

#SCUGDK

System Center User Group
Finland
#SCUGFI

Modern Management User Group
Norway
#MMUGNO

System Center User Group
Sweden
#SCUGSE



<https://2021.nordicvirtualsummit.com/feedback>