Microsoft

Microsoft Intune

Stay Compliant with M365 Compliance Score

Angela Hwa
March 2020

Confidence in the trusted cloud

- Security, privacy, compliance, risk management and intellectual property protections
- Standards and practices designed to earn confidence
- Building trust in the cloud ecosystem

Intune Compliance Offering

Global

- ISO 27001
- ISO 27018
- ISO 27017
- ISO 22301
- SOC 1 Type 2
- SOC 2 Type 2
- SOC 3
- CSA STAR Self-Assessment
- CSA STAR Certification

US Gov

- Moderate JAB P-ATO
- High JAB P-ATO
- DoD DISA SRG Level 2
- DoD DISA SRG Level 4
- SP 800-171
- FIPS 140-2
- Section 508 VPAT
- ITAR
- CJIS
- IRS 1075

Industry

- PCI DSS Level 1
- CDSA
- MPAA
- FACT UK
- Shared Assessments
- FISC Japan
- HIPAA / HITECH Act
- GxP 21 CFR Part 11
- MARS-E
- FERPA
- GLBA
- FFIEC
- HITRUST

Regional

- Argentina PDPA
- EU Model Clauses
- UK G-Cloud
- China GB 18030
- Singapore MTCS
- Australia IRAP/CCSL
- New Zealand GCIO
- Japan My Number Act
- ENISA IAF
- Japan CS Mark Gold
- Spain ENS
- Spain DPA
- India MeitY
- Canada Privacy Laws
- Privacy Shield
- Germany IT Grundschutz workbook

Achieving organizational compliance is challenging

215+

updates per day from
900 regulatory bodies[1]

"Hard to stay up-to-date to track and analyze regulatory changes."

65%

of firms ranked "design and implementation of internal processes" the biggest GDPR hurdle[2]

"Lack of in-house capabilities and connections between compliance and IT teams"

40%

of firms spent more than 4 hours a week creating and amending reports[1]

"Compliance process is highly manual, disjointed, and time-consuming."

Sources: 1 Thomson Reuters – Cost of Compliance 2018
2 http://resources.compuware.com/research-improved-gdpr-readiness-businesses-still-at-risk-of-non-compliance

Public preview

Microsoft Compliance Score

Simplify compliance and reduce risk

Continuous assessments

Detect and monitor control effectiveness automatically with a risk-based score

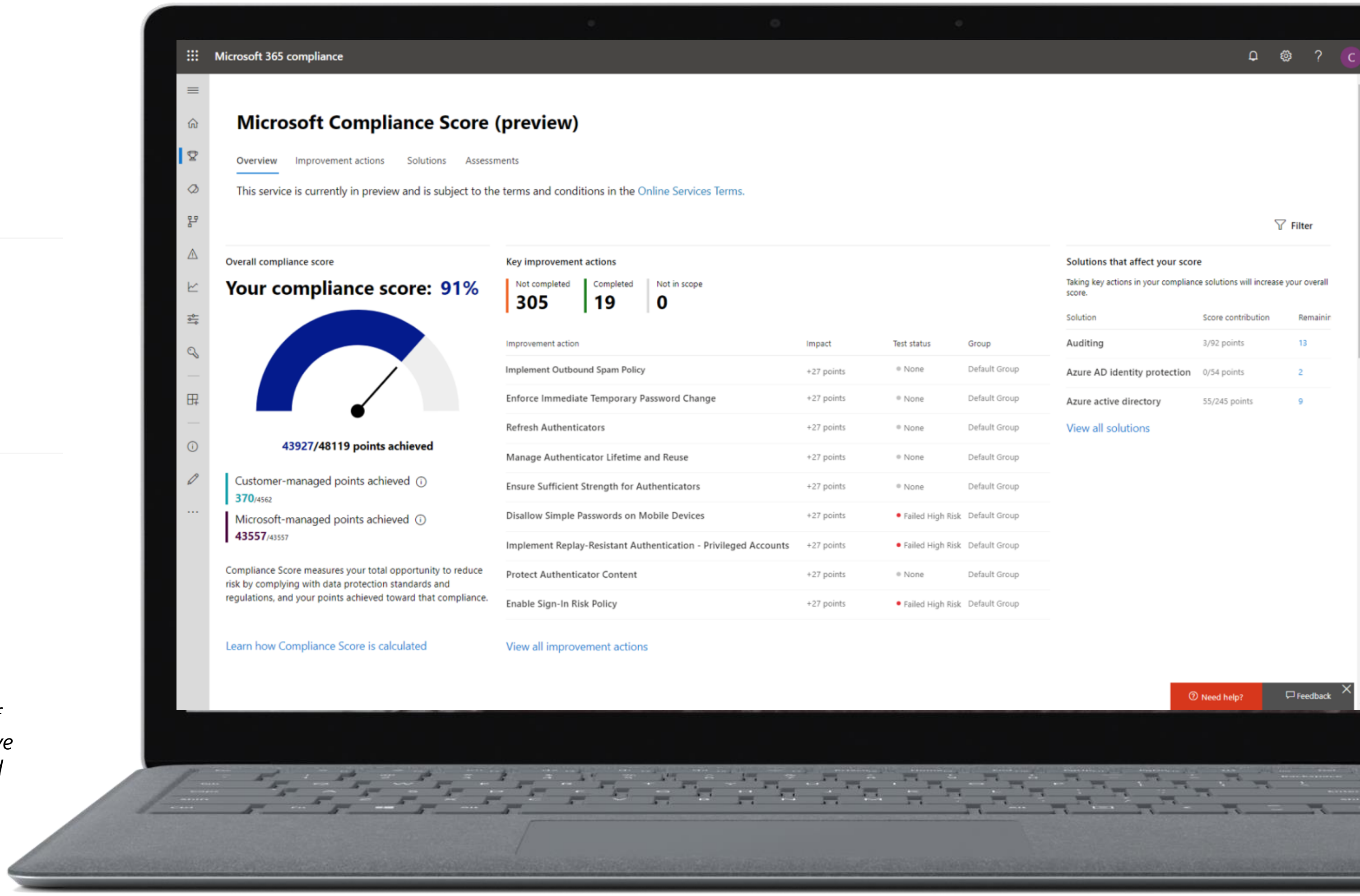
Recommended actions

Reduce compliance risks with actionable guidance

Built-in control mapping

Scale your compliance efforts with built-in mapping across regulations and standards

Compliance Score is a dashboard that provides your Compliance Score and a summary of your data protection and compliance posture. It also includes recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a guarantee of compliance.



Microsoft Compliance Score (preview)

This service is currently in preview and is subject to the terms and conditions in the Online Services Terms.

Overall compliance score

Your compliance score: 91%

43927/48119 points achieved

Customer-managed points achieved
370/4562

Microsoft-managed points achieved
43557/43557

Compliance Score measures your total opportunity to reduce risk by complying with data protection standards and regulations, and your points achieved toward that compliance.

Learn how Compliance Score is calculated

Key improvement actions

Not completed	Completed	Not in scope
305	19	0

Improvement action	Impact	Test status	Group
Implement Outbound Spam Policy	+27 points	None	Default Group
Enforce Immediate Temporary Password Change	+27 points	None	Default Group
Refresh Authenticators	+27 points	None	Default Group
Manage Authenticator Lifetime and Reuse	+27 points	None	Default Group
Ensure Sufficient Strength for Authenticators	+27 points	None	Default Group
Disallow Simple Passwords on Mobile Devices	+27 points	● Failed High Risk	Default Group
Implement Replay-Resistant Authentication - Privileged Accounts	+27 points	● Failed High Risk	Default Group
Protect Authenticator Content	+27 points	None	Default Group
Enable Sign-In Risk Policy	+27 points	● Failed High Risk	Default Group

View all improvement actions

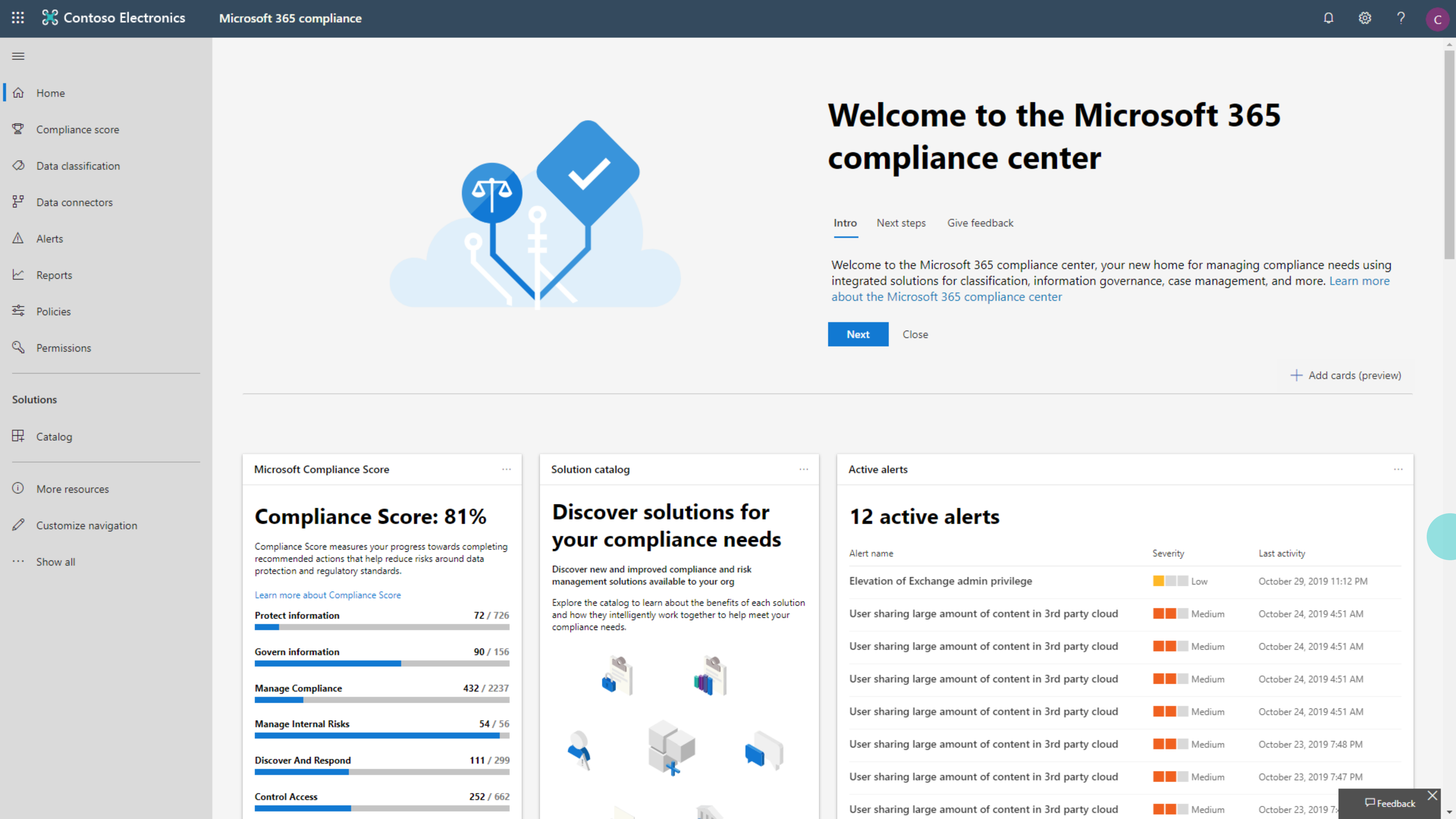
Solutions that affect your score

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

Solution	Score contribution	Remainir
Auditing	3/92 points	13
Azure AD identity protection	0/54 points	2
Azure active directory	55/245 points	9

View all solutions

Compliance Score Demo



Welcome to the Microsoft 365 compliance center

Welcome to the Microsoft 365 compliance center, your new home for managing compliance needs using integrated solutions for classification, information governance, case management, and more. Learn more about the Microsoft 365 compliance center

Microsoft Compliance Score

Compliance Score: 81%

Compliance Score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Learn more about Compliance Score

Protect information	72 / 726
Govern information	90 / 156
Manage Compliance	432 / 2237
Manage Internal Risks	54 / 56
Discover And Respond	111 / 299
Control Access	252 / 662

Solution catalog

Discover solutions for your compliance needs

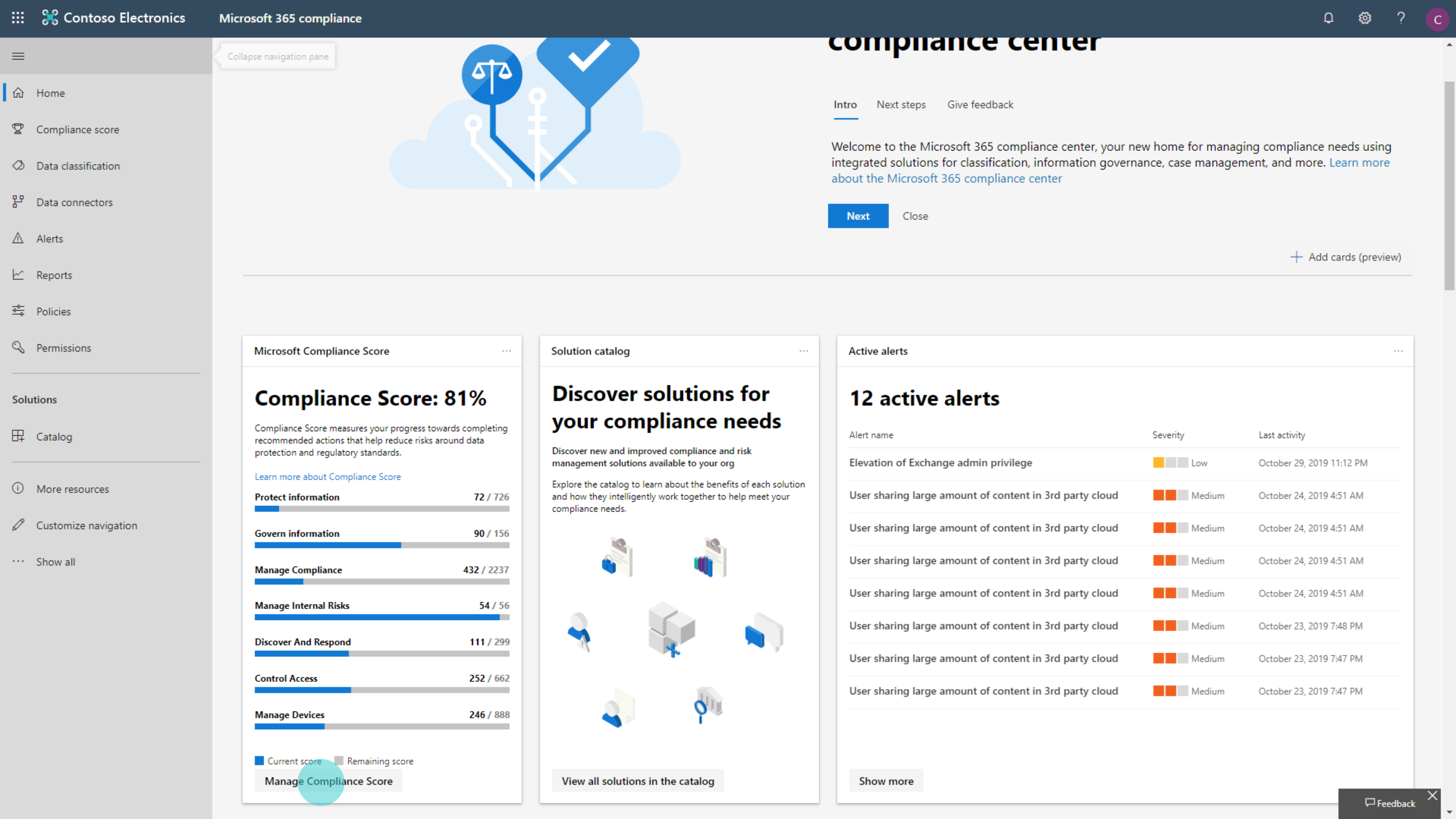
Discover new and improved compliance and risk management solutions available to your org

Explore the catalog to learn about the benefits of each solution and how they intelligently work together to help meet your compliance needs.

Active alerts

12 active alerts

Alert name	Severity	Last activity
Elevation of Exchange admin privilege	Low	October 29, 2019 11:12 PM
User sharing large amount of content in 3rd party cloud	Medium	October 24, 2019 4:51 AM
User sharing large amount of content in 3rd party cloud	Medium	October 24, 2019 4:51 AM
User sharing large amount of content in 3rd party cloud	Medium	October 24, 2019 4:51 AM
User sharing large amount of content in 3rd party cloud	Medium	October 24, 2019 4:51 AM
User sharing large amount of content in 3rd party cloud	Medium	October 23, 2019 7:48 PM
User sharing large amount of content in 3rd party cloud	Medium	October 23, 2019 7:47 PM
User sharing large amount of content in 3rd party cloud	Medium	October 23, 2019 7:



compliance center

Welcome to the Microsoft 365 compliance center, your new home for managing compliance needs using integrated solutions for classification, information governance, case management, and more. Learn more about the Microsoft 365 compliance center

Microsoft Compliance Score

Compliance Score: 81%

Compliance Score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Learn more about Compliance Score

Protect information	72 / 726
Govern information	90 / 156
Manage Compliance	432 / 2237
Manage Internal Risks	54 / 56
Discover And Respond	111 / 299
Control Access	252 / 662
Manage Devices	246 / 888

■ Current score ■ Remaining score

Manage Compliance Score

Solution catalog

Discover solutions for your compliance needs

Discover new and improved compliance and risk management solutions available to your org

Explore the catalog to learn about the benefits of each solution and how they intelligently work together to help meet your compliance needs.

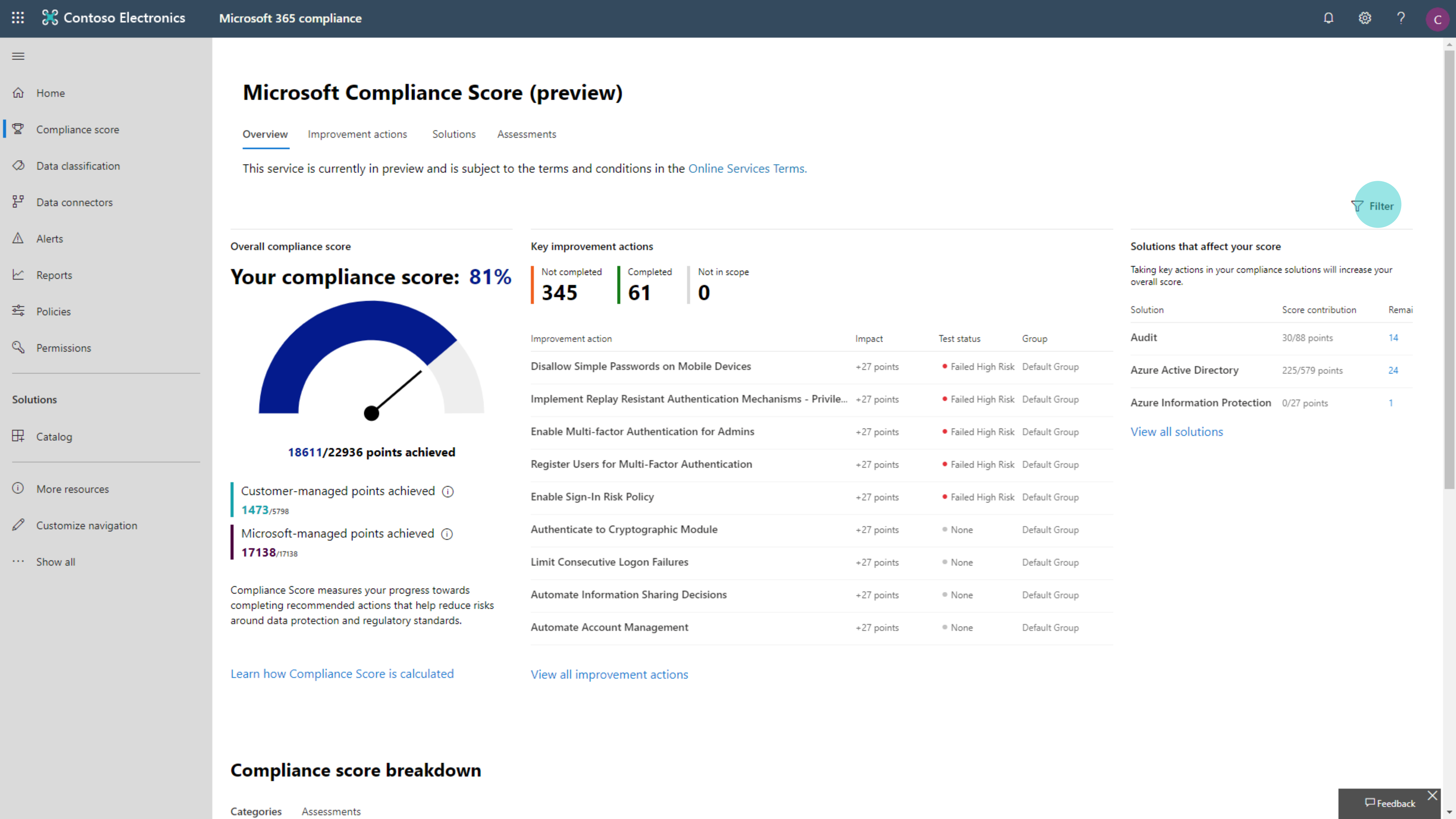
View all solutions in the catalog

Active alerts

12 active alerts

Alert name	Severity	Last activity
Elevation of Exchange admin privilege	Low	October 29, 2019 11:12 PM
User sharing large amount of content in 3rd party cloud	Medium	October 24, 2019 4:51 AM
User sharing large amount of content in 3rd party cloud	Medium	October 24, 2019 4:51 AM
User sharing large amount of content in 3rd party cloud	Medium	October 24, 2019 4:51 AM
User sharing large amount of content in 3rd party cloud	Medium	October 24, 2019 4:51 AM
User sharing large amount of content in 3rd party cloud	Medium	October 23, 2019 7:48 PM
User sharing large amount of content in 3rd party cloud	Medium	October 23, 2019 7:47 PM
User sharing large amount of content in 3rd party cloud	Medium	October 23, 2019 7:47 PM

Show more



Microsoft Compliance Score (preview)

Overview Improvement actions Solutions Assessments

This service is currently in preview and is subject to the terms and conditions in the Online Services Terms.

Overall compliance score

Your compliance score: 81%

18611/22936 points achieved

Customer-managed points achieved ⓘ
1473/5798

Microsoft-managed points achieved ⓘ
17138/17138

Compliance Score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Learn how Compliance Score is calculated

Key improvement actions

Not completed	Completed	Not in scope
345	61	0

Improvement action	Impact	Test status	Group
Disallow Simple Passwords on Mobile Devices	+27 points	● Failed High Risk	Default Group
Implement Replay Resistant Authentication Mechanisms - Privile...	+27 points	● Failed High Risk	Default Group
Enable Multi-factor Authentication for Admins	+27 points	● Failed High Risk	Default Group
Register Users for Multi-Factor Authentication	+27 points	● Failed High Risk	Default Group
Enable Sign-In Risk Policy	+27 points	● Failed High Risk	Default Group
Authenticate to Cryptographic Module	+27 points	● None	Default Group
Limit Consecutive Logon Failures	+27 points	● None	Default Group
Automate Information Sharing Decisions	+27 points	● None	Default Group
Automate Account Management	+27 points	● None	Default Group

View all improvement actions

Solutions that affect your score

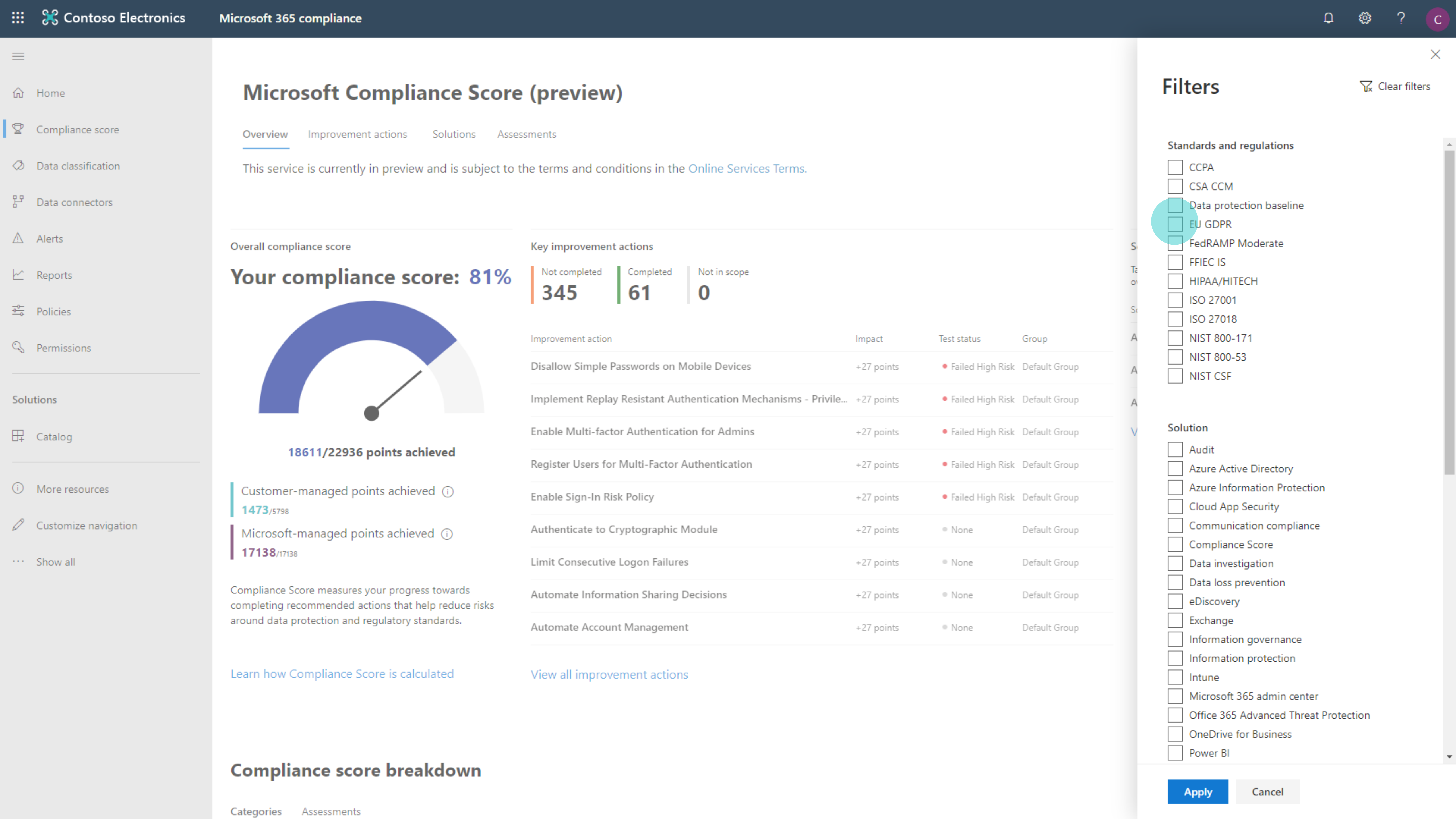
Taking key actions in your compliance solutions will increase your overall score.

Solution	Score contribution	Remai
Audit	30/88 points	14
Azure Active Directory	225/579 points	24
Azure Information Protection	0/27 points	1

View all solutions

Compliance score breakdown

Categories Assessments



Microsoft Compliance Score (preview)

This service is currently in preview and is subject to the terms and conditions in the Online Services Terms.

Overall compliance score

Your compliance score: 81%

18611/22936 points achieved

Customer-managed points achieved 1473/5798

Microsoft-managed points achieved 17138/17138

Compliance Score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Learn how Compliance Score is calculated

Key improvement actions

Not completed 345

Completed 61

Not in scope 0

Improvement action	Impact	Test status	Group
Disallow Simple Passwords on Mobile Devices	+27 points	● Failed High Risk	Default Group
Implement Replay Resistant Authentication Mechanisms - Privile...	+27 points	● Failed High Risk	Default Group
Enable Multi-factor Authentication for Admins	+27 points	● Failed High Risk	Default Group
Register Users for Multi-Factor Authentication	+27 points	● Failed High Risk	Default Group
Enable Sign-In Risk Policy	+27 points	● Failed High Risk	Default Group
Authenticate to Cryptographic Module	+27 points	● None	Default Group
Limit Consecutive Logon Failures	+27 points	● None	Default Group
Automate Information Sharing Decisions	+27 points	● None	Default Group
Automate Account Management	+27 points	● None	Default Group

View all improvement actions

Compliance score breakdown

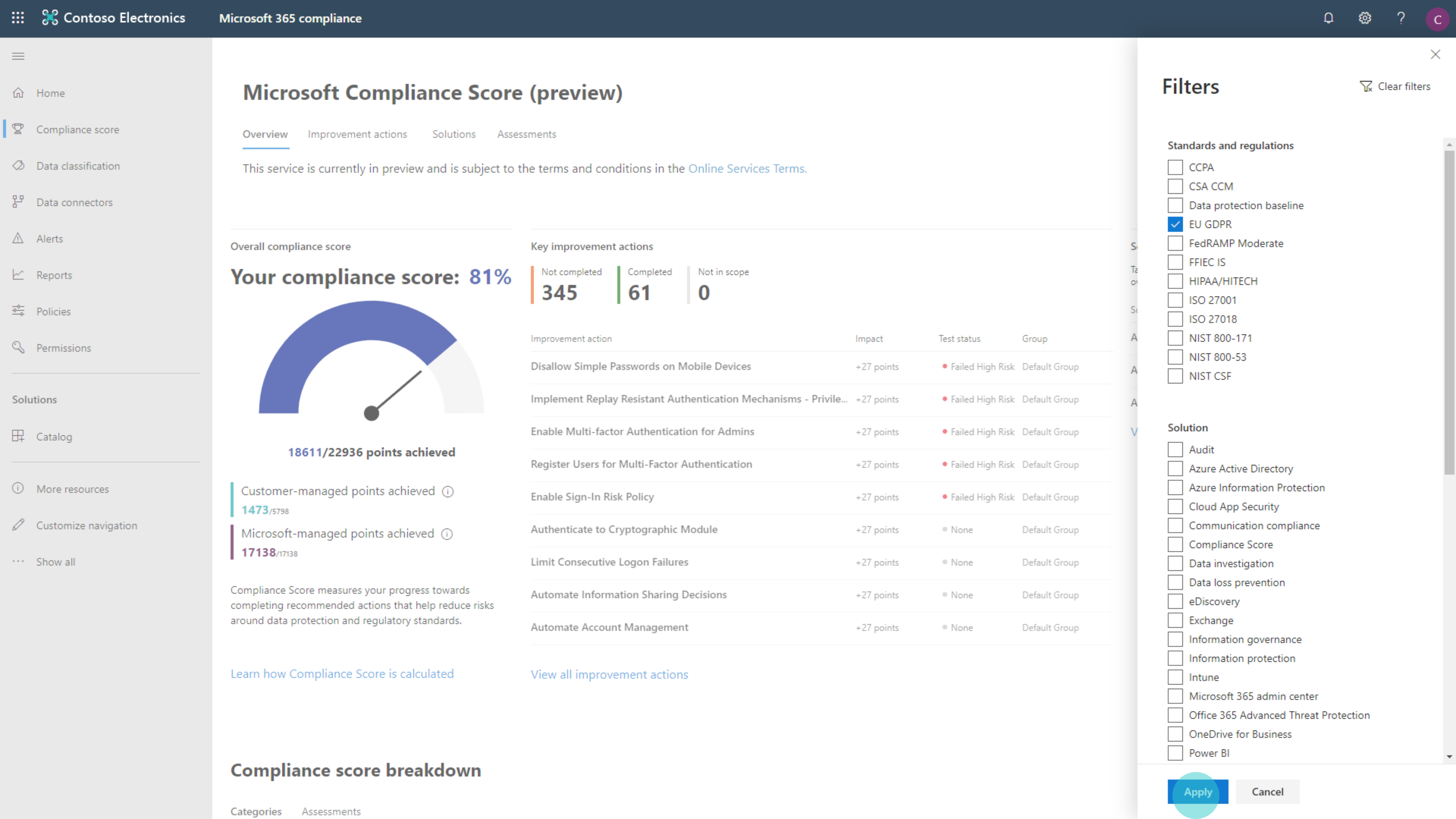
Filters

Standards and regulations

- □ CCPA
- □ CSA CCM
- □ Data protection baseline
- □ EU GDPR
- □ FedRAMP Moderate
- □ FFIEC IS
- □ HIPAA/HITECH
- □ ISO 27001
- □ ISO 27018
- □ NIST 800-171
- □ NIST 800-53
- □ NIST CSF

Solution

- □ Audit
- □ Azure Active Directory
- □ Azure Information Protection
- □ Cloud App Security
- □ Communication compliance
- □ Compliance Score
- □ Data investigation
- □ Data loss prevention
- □ eDiscovery
- □ Exchange
- □ Information governance
- □ Information protection
- □ Intune
- □ Microsoft 365 admin center
- □ Office 365 Advanced Threat Protection
- □ OneDrive for Business
- □ Power BI



Microsoft Compliance Score (preview)

This service is currently in preview and is subject to the terms and conditions in the Online Services Terms.

Overall compliance score

Your compliance score: 81%

18611/22936 points achieved

Customer-managed points achieved
1473/5798

Microsoft-managed points achieved
17138/17138

Compliance Score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Learn how Compliance Score is calculated

Key improvement actions

Not completed	Completed	Not in scope
345	61	0

Improvement action	Impact	Test status	Group
Disallow Simple Passwords on Mobile Devices	+27 points	● Failed High Risk	Default Group
Implement Replay Resistant Authentication Mechanisms - Privile...	+27 points	● Failed High Risk	Default Group
Enable Multi-factor Authentication for Admins	+27 points	● Failed High Risk	Default Group
Register Users for Multi-Factor Authentication	+27 points	● Failed High Risk	Default Group
Enable Sign-In Risk Policy	+27 points	● Failed High Risk	Default Group
Authenticate to Cryptographic Module	+27 points	● None	Default Group
Limit Consecutive Logon Failures	+27 points	● None	Default Group
Automate Information Sharing Decisions	+27 points	● None	Default Group
Automate Account Management	+27 points	● None	Default Group

View all improvement actions

Compliance score breakdown

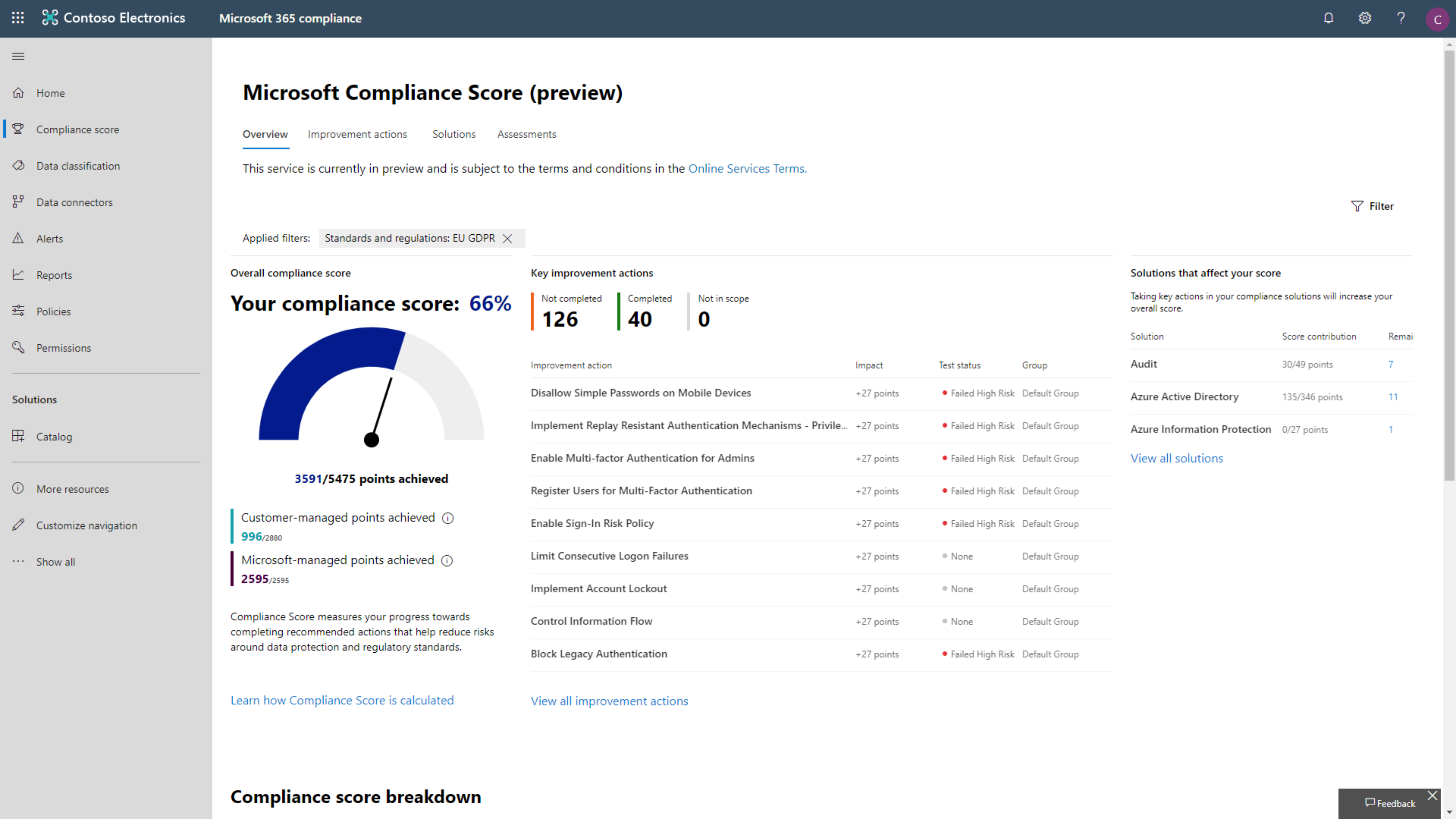
Filters

Standards and regulations

- ☐ CCPA
- ☐ CSA CCM
- ☐ Data protection baseline
- ☑ EU GDPR
- ☐ FedRAMP Moderate
- ☐ FFIEC IS
- ☐ HIPAA/HITECH
- ☐ ISO 27001
- ☐ ISO 27018
- ☐ NIST 800-171
- ☐ NIST 800-53
- ☐ NIST CSF

Solution

- ☐ Audit
- ☐ Azure Active Directory
- ☐ Azure Information Protection
- ☐ Cloud App Security
- ☐ Communication compliance
- ☐ Compliance Score
- ☐ Data investigation
- ☐ Data loss prevention
- ☐ eDiscovery
- ☐ Exchange
- ☐ Information governance
- ☐ Information protection
- ☐ Intune
- ☐ Microsoft 365 admin center
- ☐ Office 365 Advanced Threat Protection
- ☐ OneDrive for Business
- ☐ Power BI



Microsoft Compliance Score (preview)

This service is currently in preview and is subject to the terms and conditions in the Online Services Terms.

Applied filters: Standards and regulations: EU GDPR

Overall compliance score

Your compliance score: 66%

3591/5475 points achieved

Customer-managed points achieved
996/2880

Microsoft-managed points achieved
2595/2595

Compliance Score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Learn how Compliance Score is calculated

Key improvement actions

Not completed	Completed	Not in scope
126	40	0

Improvement action	Impact	Test status	Group
Disallow Simple Passwords on Mobile Devices	+27 points	● Failed High Risk	Default Group
Implement Replay Resistant Authentication Mechanisms - Privile...	+27 points	● Failed High Risk	Default Group
Enable Multi-factor Authentication for Admins	+27 points	● Failed High Risk	Default Group
Register Users for Multi-Factor Authentication	+27 points	● Failed High Risk	Default Group
Enable Sign-In Risk Policy	+27 points	● Failed High Risk	Default Group
Limit Consecutive Logon Failures	+27 points	● None	Default Group
Implement Account Lockout	+27 points	● None	Default Group
Control Information Flow	+27 points	● None	Default Group
Block Legacy Authentication	+27 points	● Failed High Risk	Default Group

View all improvement actions

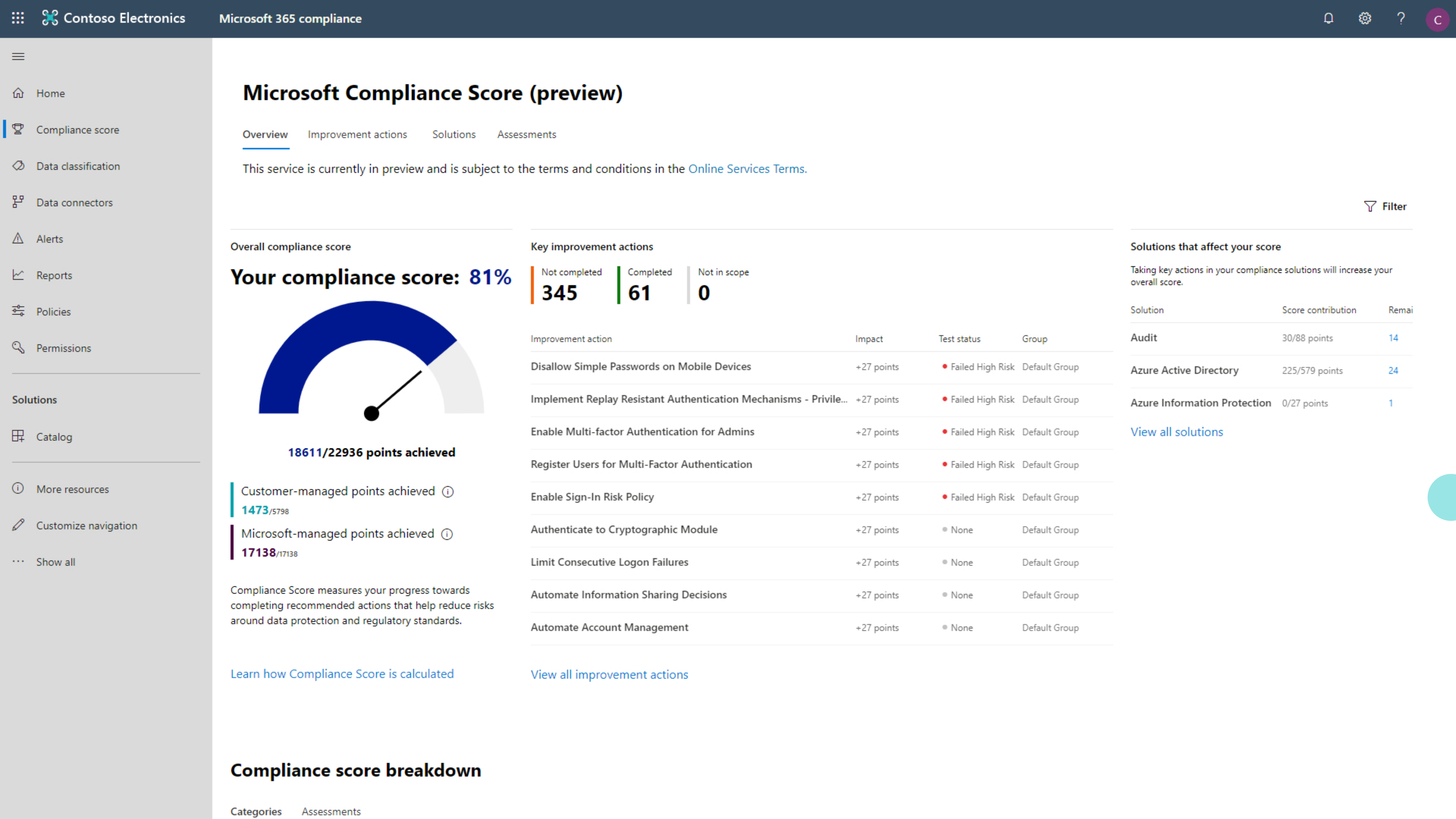
Solutions that affect your score

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

Solution	Score contribution	Remai
Audit	30/49 points	7
Azure Active Directory	135/346 points	11
Azure Information Protection	0/27 points	1

View all solutions

Compliance score breakdown



Microsoft Compliance Score (preview)

Overview | Improvement actions | Solutions | Assessments

This service is currently in preview and is subject to the terms and conditions in the Online Services Terms.

Overall compliance score

Your compliance score: 81%

18611/22936 points achieved

Customer-managed points achieved ⓘ
1473/5798

Microsoft-managed points achieved ⓘ
17138/17138

Compliance Score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Learn how Compliance Score is calculated

Key improvement actions

Not completed	Completed	Not in scope
345	61	0

Improvement action	Impact	Test status	Group
Disallow Simple Passwords on Mobile Devices	+27 points	● Failed High Risk	Default Group
Implement Replay Resistant Authentication Mechanisms - Privile...	+27 points	● Failed High Risk	Default Group
Enable Multi-factor Authentication for Admins	+27 points	● Failed High Risk	Default Group
Register Users for Multi-Factor Authentication	+27 points	● Failed High Risk	Default Group
Enable Sign-In Risk Policy	+27 points	● Failed High Risk	Default Group
Authenticate to Cryptographic Module	+27 points	● None	Default Group
Limit Consecutive Logon Failures	+27 points	● None	Default Group
Automate Information Sharing Decisions	+27 points	● None	Default Group
Automate Account Management	+27 points	● None	Default Group

View all improvement actions

Solutions that affect your score

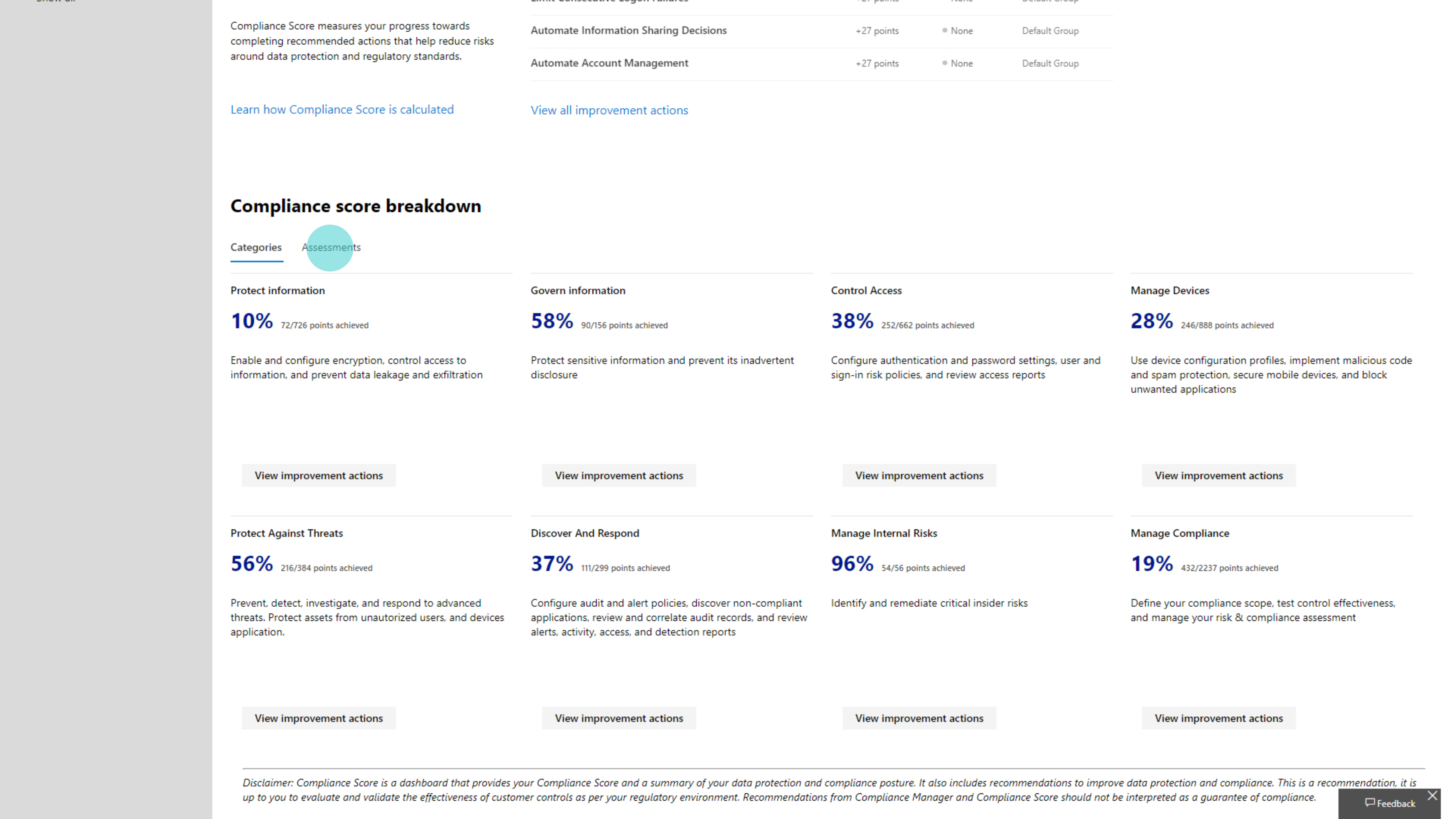
Taking key actions in your compliance solutions will increase your overall score.

Solution	Score contribution	Remai
Audit	30/88 points	14
Azure Active Directory	225/579 points	24
Azure Information Protection	0/27 points	1

View all solutions

Compliance score breakdown

Categories | Assessments



Compliance Score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Learn how Compliance Score is calculated

Limit Consecutive Logon Failures	+27 points	● None	Default Group
Automate Information Sharing Decisions	+27 points	● None	Default Group
Automate Account Management	+27 points	● None	Default Group

View all improvement actions

Compliance score breakdown

Protect information

10% 72/726 points achieved

Enable and configure encryption, control access to information, and prevent data leakage and exfiltration

Govern information

58% 90/156 points achieved

Protect sensitive information and prevent its inadvertent disclosure

Control Access

38% 252/662 points achieved

Configure authentication and password settings, user and sign-in risk policies, and review access reports

Manage Devices

28% 246/888 points achieved

Use device configuration profiles, implement malicious code and spam protection, secure mobile devices, and block unwanted applications

Protect Against Threats

56% 216/384 points achieved

Prevent, detect, investigate, and respond to advanced threats. Protect assets from unautorized users, and devices application.

Discover And Respond

37% 111/299 points achieved

Configure audit and alert policies, discover non-compliant applications, review and correlate audit records, and review alerts, activity, access, and detection reports

Manage Internal Risks

96% 54/56 points achieved

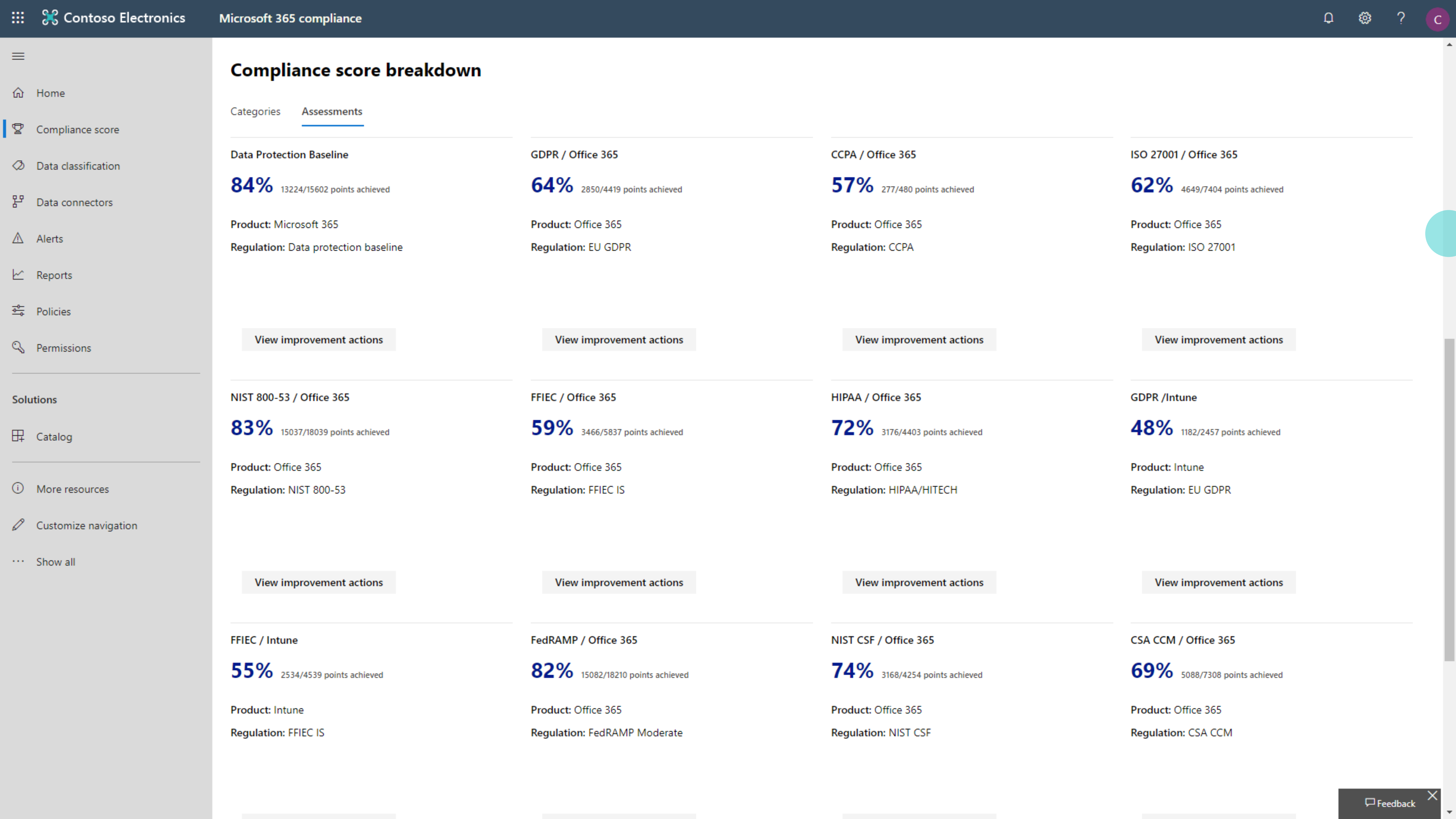
Identify and remediate critical insider risks

Manage Compliance

19% 432/2237 points achieved

Define your compliance scope, test control effectiveness, and manage your risk & compliance assessment

Disclaimer: Compliance Score is a dashboard that provides your Compliance Score and a summary of your data protection and compliance posture. It also includes recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a guarantee of compliance.



Compliance score breakdown

Categories | Assessments

Data Protection Baseline

84% 13224/15602 points achieved

Product: Microsoft 365

Regulation: Data protection baseline

View improvement actions

GDPR / Office 365

64% 2850/4419 points achieved

Product: Office 365

Regulation: EU GDPR

View improvement actions

CCPA / Office 365

57% 277/480 points achieved

Product: Office 365

Regulation: CCPA

View improvement actions

ISO 27001 / Office 365

62% 4649/7404 points achieved

Product: Office 365

Regulation: ISO 27001

View improvement actions

NIST 800-53 / Office 365

83% 15037/18039 points achieved

Product: Office 365

Regulation: NIST 800-53

View improvement actions

FFIEC / Office 365

59% 3466/5837 points achieved

Product: Office 365

Regulation: FFIEC IS

View improvement actions

HIPAA / Office 365

72% 3176/4403 points achieved

Product: Office 365

Regulation: HIPAA/HITECH

View improvement actions

GDPR /Intune

48% 1182/2457 points achieved

Product: Intune

Regulation: EU GDPR

View improvement actions

FFIEC / Intune

55% 2534/4539 points achieved

Product: Intune

Regulation: FFIEC IS

FedRAMP / Office 365

82% 15082/18210 points achieved

Product: Office 365

Regulation: FedRAMP Moderate

NIST CSF / Office 365

74% 3168/4254 points achieved

Product: Office 365

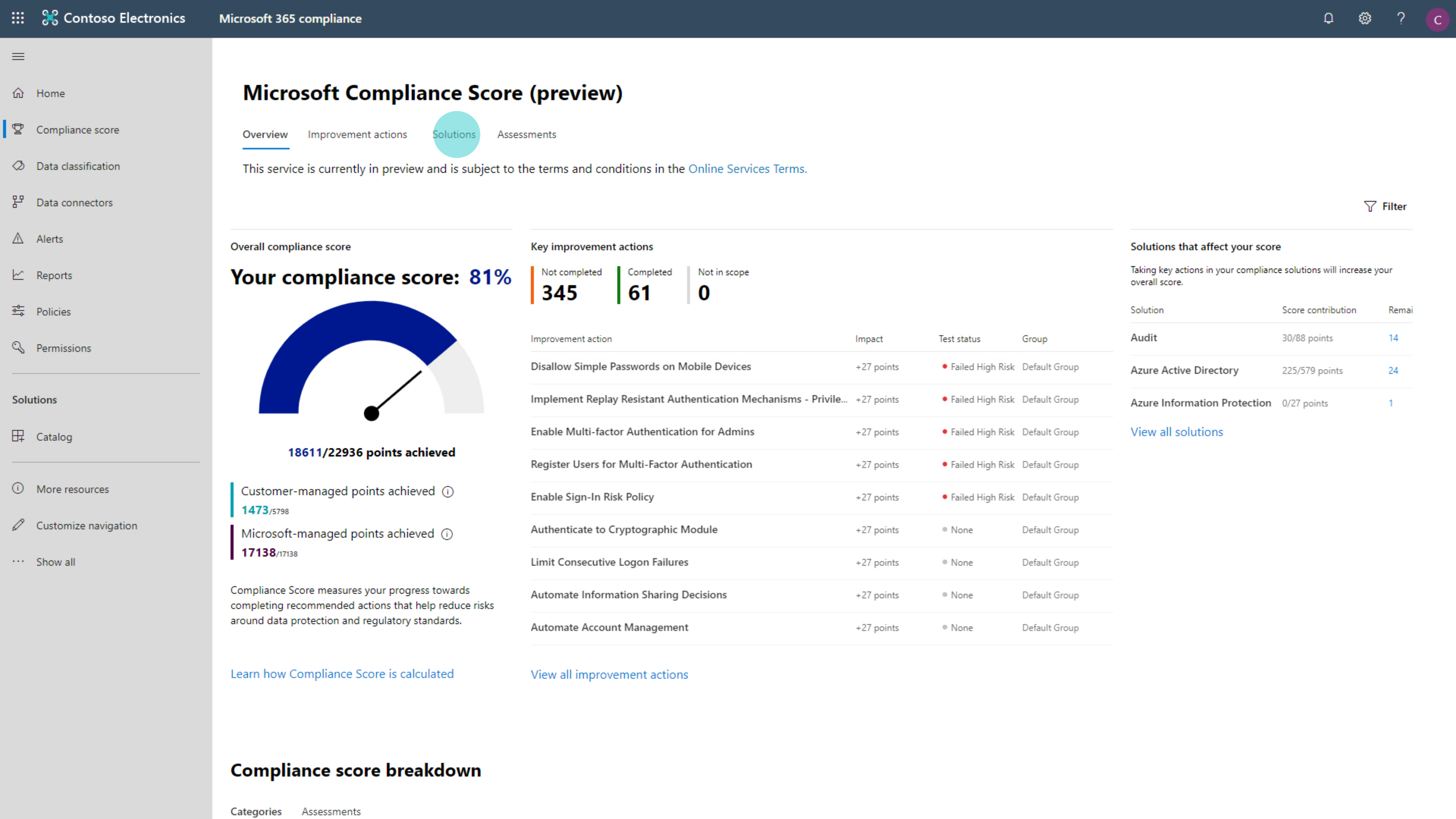
Regulation: NIST CSF

CSA CCM / Office 365

69% 5088/7308 points achieved

Product: Office 365

Regulation: CSA CCM



Microsoft Compliance Score (preview)

Overview | Improvement actions | Solutions | Assessments

This service is currently in preview and is subject to the terms and conditions in the Online Services Terms.

Overall compliance score

Your compliance score: 81%

18611/22936 points achieved

Customer-managed points achieved ⓘ
1473/5798

Microsoft-managed points achieved ⓘ
17138/17138

Compliance Score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Learn how Compliance Score is calculated

Key improvement actions

Not completed	Completed	Not in scope
345	61	0

Improvement action	Impact	Test status	Group
Disallow Simple Passwords on Mobile Devices	+27 points	● Failed High Risk	Default Group
Implement Replay Resistant Authentication Mechanisms - Privile...	+27 points	● Failed High Risk	Default Group
Enable Multi-factor Authentication for Admins	+27 points	● Failed High Risk	Default Group
Register Users for Multi-Factor Authentication	+27 points	● Failed High Risk	Default Group
Enable Sign-In Risk Policy	+27 points	● Failed High Risk	Default Group
Authenticate to Cryptographic Module	+27 points	● None	Default Group
Limit Consecutive Logon Failures	+27 points	● None	Default Group
Automate Information Sharing Decisions	+27 points	● None	Default Group
Automate Account Management	+27 points	● None	Default Group

View all improvement actions

Solutions that affect your score

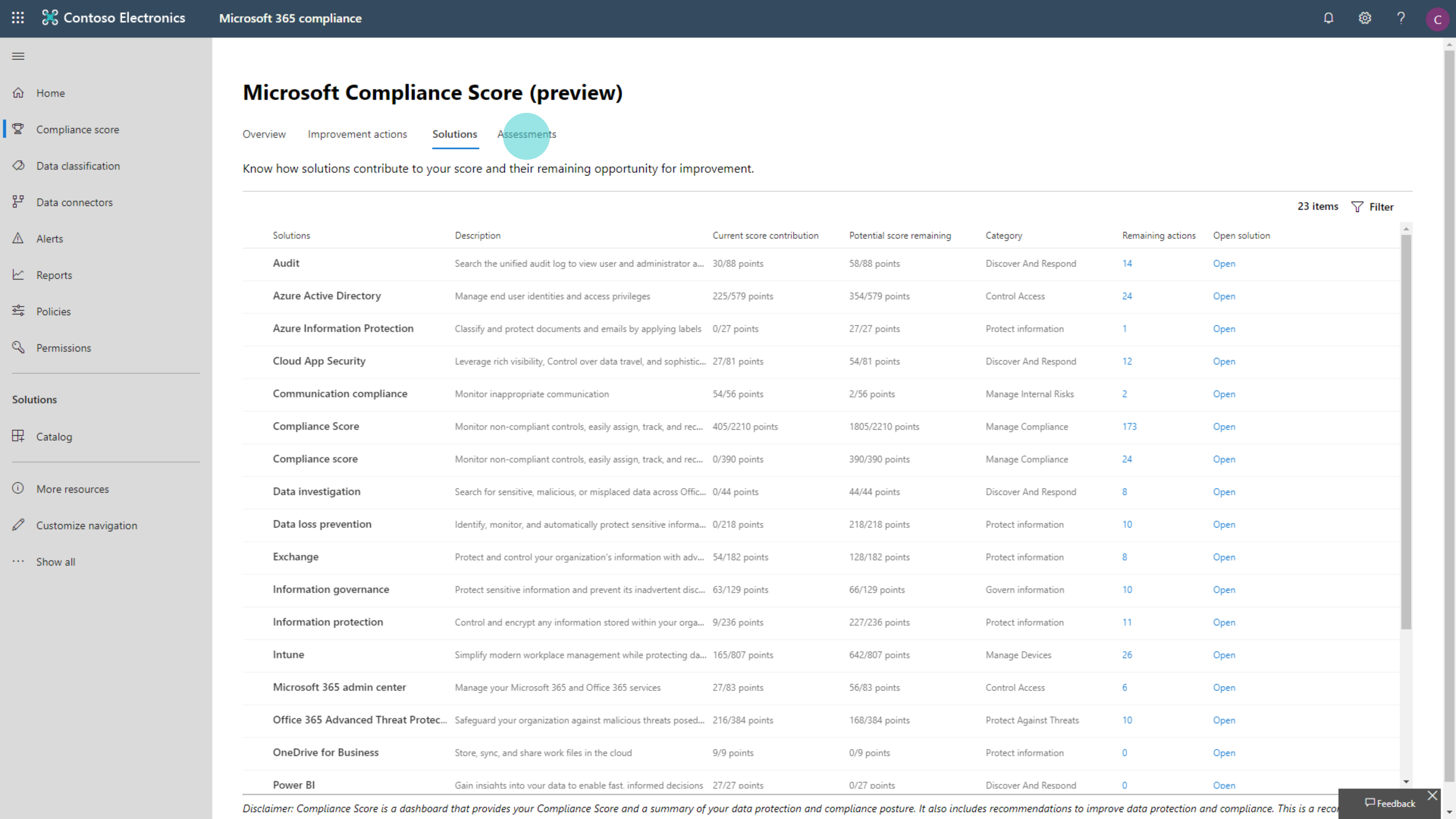
Taking key actions in your compliance solutions will increase your overall score.

Solution	Score contribution	Remai
Audit	30/88 points	14
Azure Active Directory	225/579 points	24
Azure Information Protection	0/27 points	1

View all solutions

Compliance score breakdown

Categories | Assessments

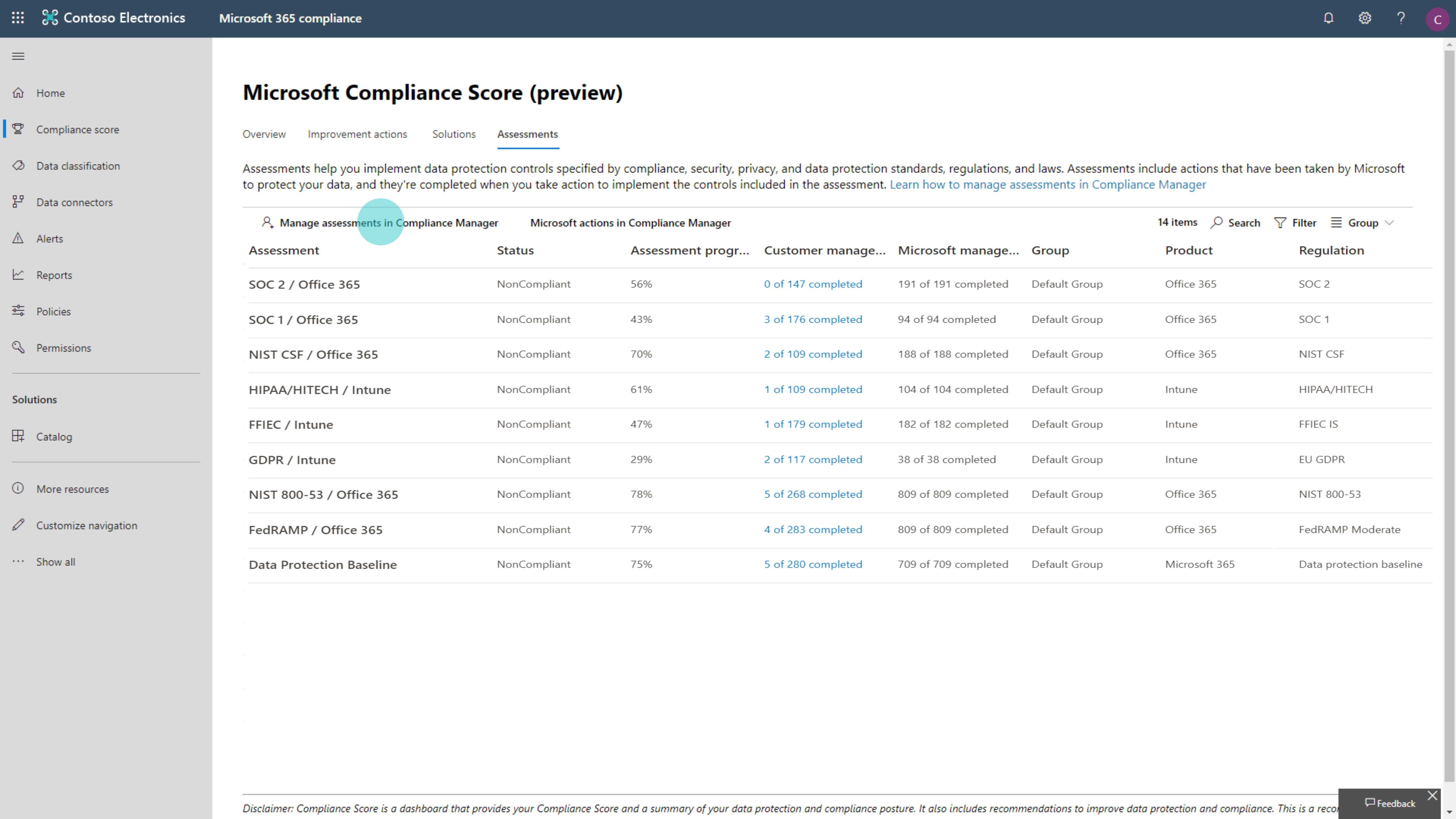


Microsoft Compliance Score (preview)

Know how solutions contribute to your score and their remaining opportunity for improvement.

Solutions	Description	Current score contribution	Potential score remaining	Category	Remaining actions	Open solution
Audit	Search the unified audit log to view user and administrator a...	30/88 points	58/88 points	Discover And Respond	14	Open
Azure Active Directory	Manage end user identities and access privileges	225/579 points	354/579 points	Control Access	24	Open
Azure Information Protection	Classify and protect documents and emails by applying labels	0/27 points	27/27 points	Protect information	1	Open
Cloud App Security	Leverage rich visibility, Control over data travel, and sophistic...	27/81 points	54/81 points	Discover And Respond	12	Open
Communication compliance	Monitor inappropriate communication	54/56 points	2/56 points	Manage Internal Risks	2	Open
Compliance Score	Monitor non-compliant controls, easily assign, track, and rec...	405/2210 points	1805/2210 points	Manage Compliance	173	Open
Compliance score	Monitor non-compliant controls, easily assign, track, and rec...	0/390 points	390/390 points	Manage Compliance	24	Open
Data investigation	Search for sensitive, malicious, or misplaced data across Offic...	0/44 points	44/44 points	Discover And Respond	8	Open
Data loss prevention	Identify, monitor, and automatically protect sensitive informa...	0/218 points	218/218 points	Protect information	10	Open
Exchange	Protect and control your organization's information with adv...	54/182 points	128/182 points	Protect information	8	Open
Information governance	Protect sensitive information and prevent its inadvertent disc...	63/129 points	66/129 points	Govern information	10	Open
Information protection	Control and encrypt any information stored within your orga...	9/236 points	227/236 points	Protect information	11	Open
Intune	Simplify modern workplace management while protecting da...	165/807 points	642/807 points	Manage Devices	26	Open
Microsoft 365 admin center	Manage your Microsoft 365 and Office 365 services	27/83 points	56/83 points	Control Access	6	Open
Office 365 Advanced Threat Protec...	Safeguard your organization against malicious threats posed...	216/384 points	168/384 points	Protect Against Threats	10	Open
OneDrive for Business	Store, sync, and share work files in the cloud	9/9 points	0/9 points	Protect information	0	Open
Power BI	Gain insights into your data to enable fast, informed decisions	27/27 points	0/27 points	Discover And Respond	0	Open

Disclaimer: Compliance Score is a dashboard that provides your Compliance Score and a summary of your data protection and compliance posture. It also includes recommendations to improve data protection and compliance. This is a reco

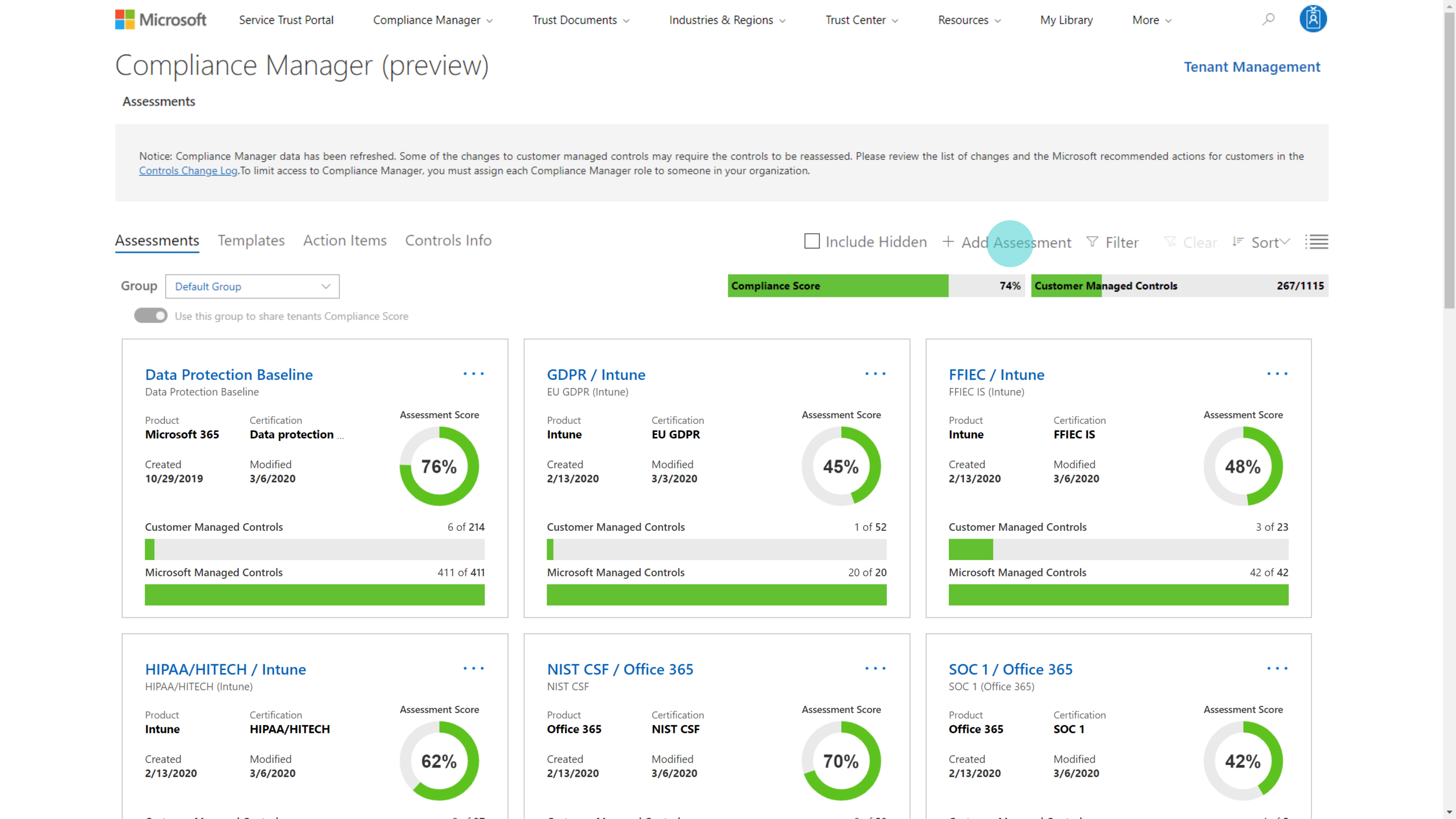


Microsoft Compliance Score (preview)

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

Assessment	Status	Assessment progr...	Customer manage...	Microsoft manage...	Group	Product	Regulation
SOC 2 / Office 365	NonCompliant	56%	0 of 147 completed	191 of 191 completed	Default Group	Office 365	SOC 2
SOC 1 / Office 365	NonCompliant	43%	3 of 176 completed	94 of 94 completed	Default Group	Office 365	SOC 1
NIST CSF / Office 365	NonCompliant	70%	2 of 109 completed	188 of 188 completed	Default Group	Office 365	NIST CSF
HIPAA/HITECH / Intune	NonCompliant	61%	1 of 109 completed	104 of 104 completed	Default Group	Intune	HIPAA/HITECH
FFIEC / Intune	NonCompliant	47%	1 of 179 completed	182 of 182 completed	Default Group	Intune	FFIEC IS
GDPR / Intune	NonCompliant	29%	2 of 117 completed	38 of 38 completed	Default Group	Intune	EU GDPR
NIST 800-53 / Office 365	NonCompliant	78%	5 of 268 completed	809 of 809 completed	Default Group	Office 365	NIST 800-53
FedRAMP / Office 365	NonCompliant	77%	4 of 283 completed	809 of 809 completed	Default Group	Office 365	FedRAMP Moderate
Data Protection Baseline	NonCompliant	75%	5 of 280 completed	709 of 709 completed	Default Group	Microsoft 365	Data protection baseline

Disclaimer: Compliance Score is a dashboard that provides your Compliance Score and a summary of your data protection and compliance posture. It also includes recommendations to improve data protection and compliance. This is a reco



Microsoft Service Trust Portal Compliance Manager ⌄ Trust Documents ⌄ Industries & Regions ⌄ Trust Center ⌄ Resources ⌄ My Library More ⌄

Compliance Manager (preview)

Tenant Management

Assessments

Notice: Compliance Manager data has been refreshed. Some of the changes to customer managed controls may require the controls to be reassessed. Please review the list of changes and the Microsoft recommended actions for customers in the Controls Change Log.To limit access to Compliance Manager, you must assign each Compliance Manager role to someone in your organization.

Assessments Templates Action Items Controls Info

□ Include Hidden + Add Assessment Filter Clear Sort⌄

Group Default Group ⌄

Use this group to share tenants Compliance Score

Compliance Score 74%

Customer Managed Controls 267/1115

Data Protection Baseline • • •
Data Protection Baseline

Product	Certification	Assessment Score
Microsoft 365	Data protection ...	76%
Created 10/29/2019	Modified 3/6/2020	

Customer Managed Controls 6 of 214

Microsoft Managed Controls 411 of 411

GDPR / Intune • • •
EU GDPR (Intune)

Product	Certification	Assessment Score
Intune	EU GDPR	45%
Created 2/13/2020	Modified 3/3/2020	

Customer Managed Controls 1 of 52

Microsoft Managed Controls 20 of 20

FFIEC / Intune • • •
FFIEC IS (Intune)

Product	Certification	Assessment Score
Intune	FFIEC IS	48%
Created 2/13/2020	Modified 3/6/2020	

Customer Managed Controls 3 of 23

Microsoft Managed Controls 42 of 42

HIPAA/HITECH / Intune • • •
HIPAA/HITECH (Intune)

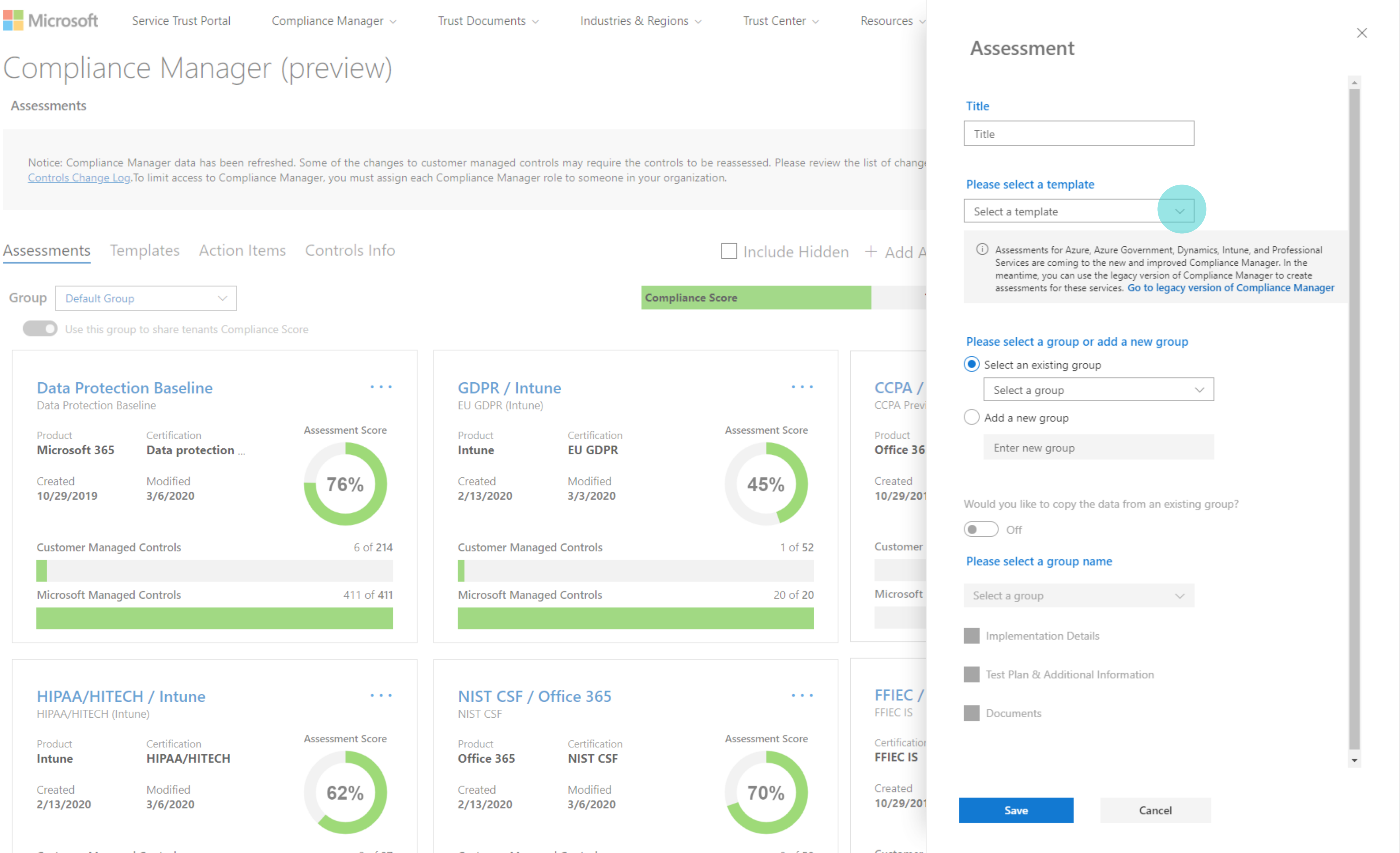
Product	Certification	Assessment Score
Intune	HIPAA/HITECH	62%
Created 2/13/2020	Modified 3/6/2020	

NIST CSF / Office 365 • • •
NIST CSF

Product	Certification	Assessment Score
Office 365	NIST CSF	70%
Created 2/13/2020	Modified 3/6/2020	

SOC 1 / Office 365 • • •
SOC 1 (Office 365)

Product	Certification	Assessment Score
Office 365	SOC 1	42%
Created 2/13/2020	Modified 3/6/2020	



Microsoft | Service Trust Portal | Compliance Manager ⌵ | Trust Documents ⌵ | Industries & Regions ⌵ | Trust Center ⌵ | Resources ⌵

Compliance Manager (preview)

Assessments

Notice: Compliance Manager data has been refreshed. Some of the changes to customer managed controls may require the controls to be reassessed. Please review the list of chang
Controls Change Log.To limit access to Compliance Manager, you must assign each Compliance Manager role to someone in your organization.

Assessments | Templates | Action Items | Controls Info | □ Include Hidden | + Add A

Group: Default Group ⌵

Use this group to share tenants Compliance Score

Compliance Score

Data Protection Baseline ···
Data Protection Baseline
Product: Microsoft 365
Certification: Data protection ...
Created: 10/29/2019
Modified: 3/6/2020
Assessment Score: 76%
Customer Managed Controls: 6 of 214
Microsoft Managed Controls: 411 of 411

GDPR / Intune ···
EU GDPR (Intune)
Product: Intune
Certification: EU GDPR
Created: 2/13/2020
Modified: 3/3/2020
Assessment Score: 45%
Customer Managed Controls: 1 of 52
Microsoft Managed Controls: 20 of 20

CCPA /
CCPA Prev
Product: Office 36
Created: 10/29/201
Customer
Microsoft

HIPAA/HITECH / Intune ···
HIPAA/HITECH (Intune)
Product: Intune
Certification: HIPAA/HITECH
Created: 2/13/2020
Modified: 3/6/2020
Assessment Score: 62%

NIST CSF / Office 365 ···
NIST CSF
Product: Office 365
Certification: NIST CSF
Created: 2/13/2020
Modified: 3/6/2020
Assessment Score: 70%

FFIEC /
FFIEC IS
Certificatio: FFIEC IS
Created: 10/29/201

Assessment

Title: Title

Please select a template: Select a template ⌵

ⓘ Assessments for Azure, Azure Government, Dynamics, Intune, and Professional Services are coming to the new and improved Compliance Manager. In the meantime, you can use the legacy version of Compliance Manager to create assessments for these services. Go to legacy version of Compliance Manager

Please select a group or add a new group

● Select an existing group: Select a group ⌵

○ Add a new group: Enter new group

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

Off

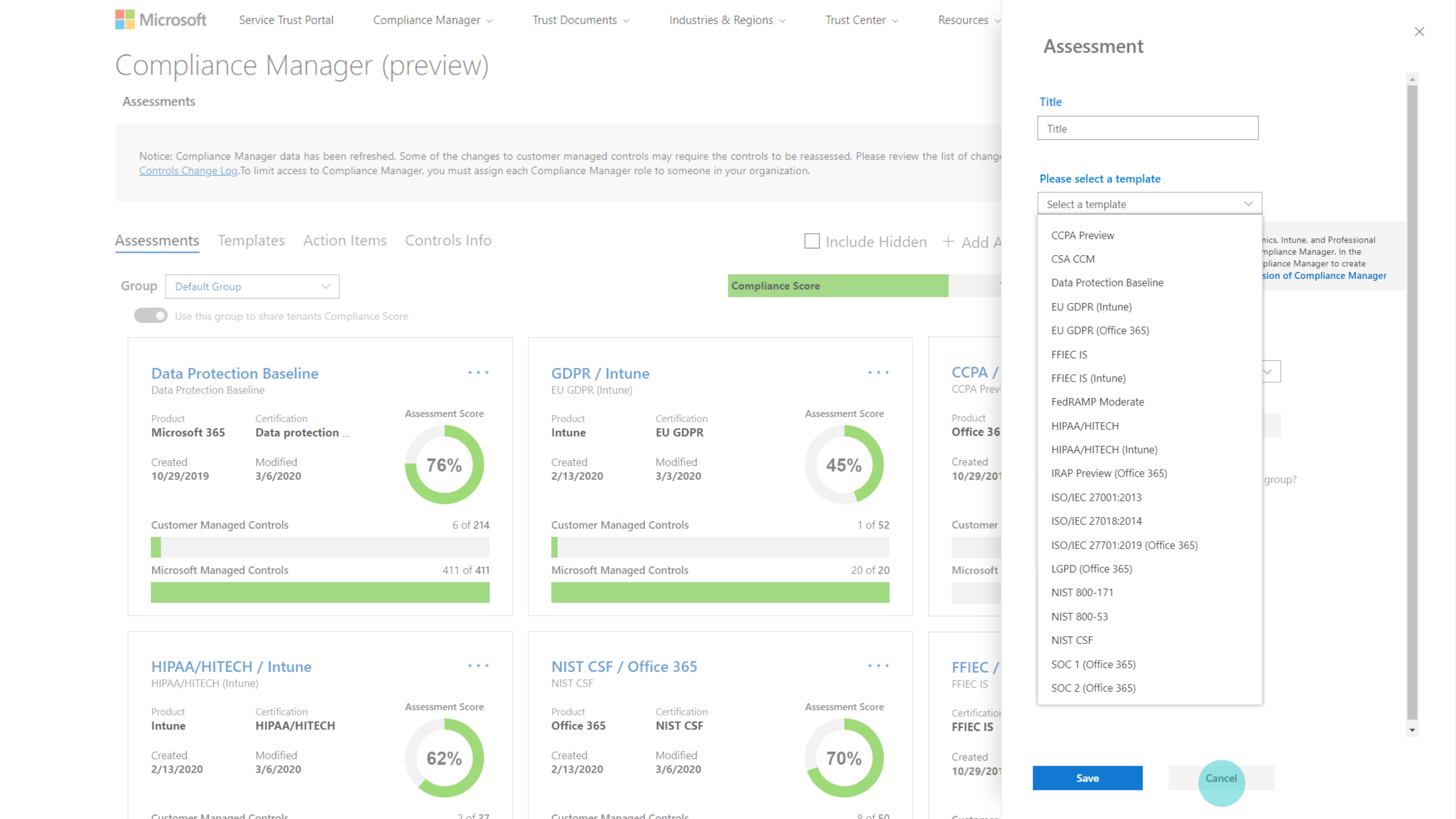
Please select a group name: Select a group ⌵

□ Implementation Details

□ Test Plan & Additional Information

□ Documents

Save | Cancel



Microsoft | Service Trust Portal | Compliance Manager | Trust Documents | Industries & Regions | Trust Center | Resources

Compliance Manager (preview)

Assessments

Notice: Compliance Manager data has been refreshed. Some of the changes to customer managed controls may require the controls to be reassessed. Please review the list of chang
Controls Change Log.To limit access to Compliance Manager, you must assign each Compliance Manager role to someone in your organization.

Assessments | Templates | Action Items | Controls Info

□ Include Hidden + Add A

Group: Default Group

Use this group to share tenants Compliance Score

Compliance Score

Data Protection Baseline
Data Protection Baseline
Product: Microsoft 365
Certification: Data protection ...
Created: 10/29/2019
Modified: 3/6/2020
Assessment Score: 76%
Customer Managed Controls: 6 of 214
Microsoft Managed Controls: 411 of 411

GDPR / Intune
EU GDPR (Intune)
Product: Intune
Certification: EU GDPR
Created: 2/13/2020
Modified: 3/3/2020
Assessment Score: 45%
Customer Managed Controls: 1 of 52
Microsoft Managed Controls: 20 of 20

CCPA /
CCPA Previ
Product: Office 36
Created: 10/29/201
Customer
Microsoft

HIPAA/HITECH / Intune
HIPAA/HITECH (Intune)
Product: Intune
Certification: HIPAA/HITECH
Created: 2/13/2020
Modified: 3/6/2020
Assessment Score: 62%
Customer Managed Controls: 2 of 37

NIST CSF / Office 365
NIST CSF
Product: Office 365
Certification: NIST CSF
Created: 2/13/2020
Modified: 3/6/2020
Assessment Score: 70%
Customer Managed Controls: 8 of 50

FFIEC /
FFIEC IS
Certificatio: FFIEC IS
Created: 10/29/201

Assessment

Title: Title

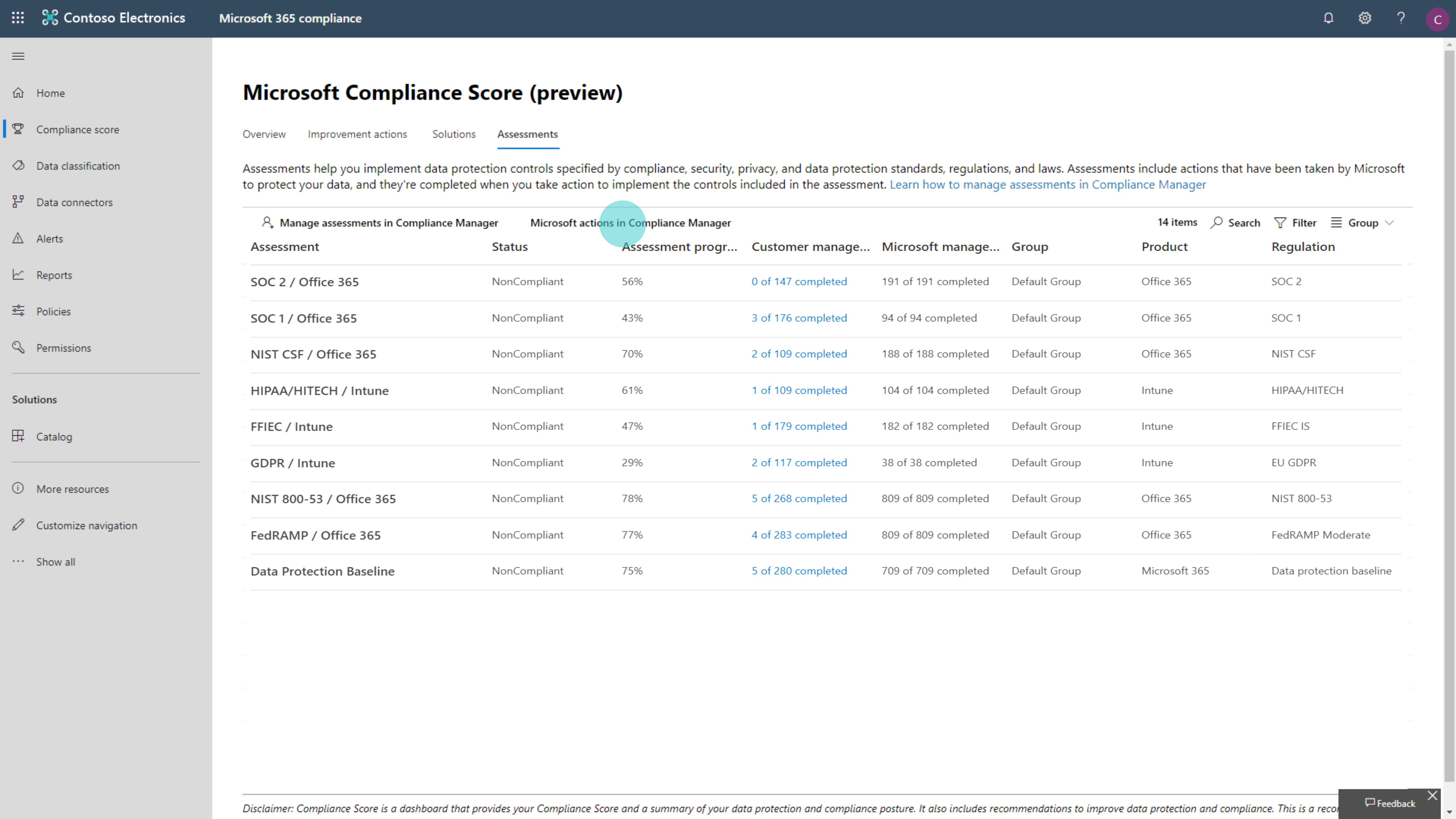
Please select a template: Select a template

- CCPA Preview
- CSA CCM
- Data Protection Baseline
- EU GDPR (Intune)
- EU GDPR (Office 365)
- FFIEC IS
- FFIEC IS (Intune)
- FedRAMP Moderate
- HIPAA/HITECH
- HIPAA/HITECH (Intune)
- IRAP Preview (Office 365)
- ISO/IEC 27001:2013
- ISO/IEC 27018:2014
- ISO/IEC 27701:2019 (Office 365)
- LGPD (Office 365)
- NIST 800-171
- NIST 800-53
- NIST CSF
- SOC 1 (Office 365)
- SOC 2 (Office 365)

nics, Intune, and Professional
mpliance Manager. In the
pliance Manager to create
sion of Compliance Manager

group?

Save | Cancel



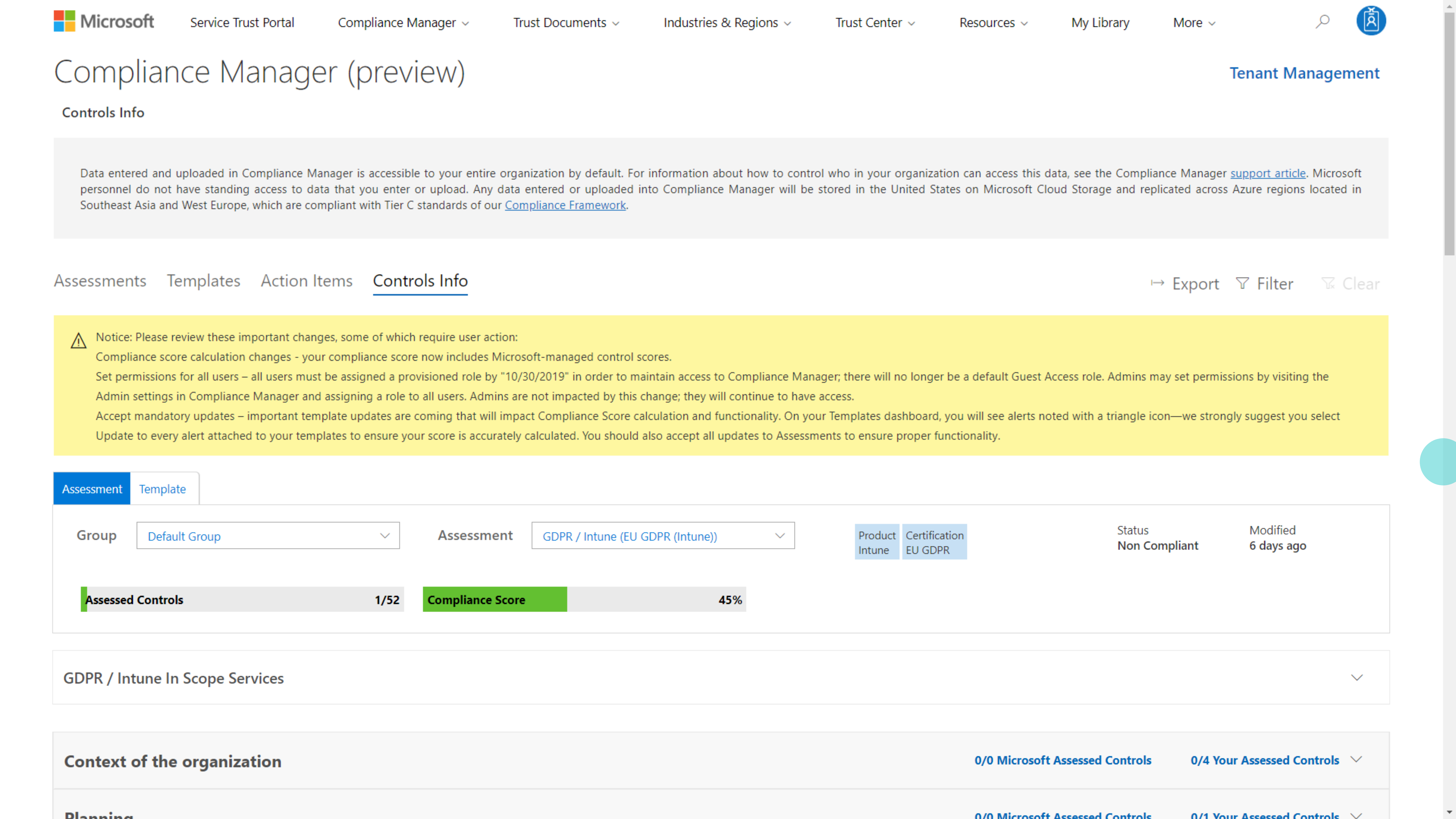
Microsoft Compliance Score (preview)

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

Manage assessments in Compliance Manager
Microsoft actions in Compliance Manager
14 items
Search
Filter
Group

Assessment	Status	Assessment progr...	Customer manage...	Microsoft manage...	Group	Product	Regulation
SOC 2 / Office 365	NonCompliant	56%	0 of 147 completed	191 of 191 completed	Default Group	Office 365	SOC 2
SOC 1 / Office 365	NonCompliant	43%	3 of 176 completed	94 of 94 completed	Default Group	Office 365	SOC 1
NIST CSF / Office 365	NonCompliant	70%	2 of 109 completed	188 of 188 completed	Default Group	Office 365	NIST CSF
HIPAA/HITECH / Intune	NonCompliant	61%	1 of 109 completed	104 of 104 completed	Default Group	Intune	HIPAA/HITECH
FFIEC / Intune	NonCompliant	47%	1 of 179 completed	182 of 182 completed	Default Group	Intune	FFIEC IS
GDPR / Intune	NonCompliant	29%	2 of 117 completed	38 of 38 completed	Default Group	Intune	EU GDPR
NIST 800-53 / Office 365	NonCompliant	78%	5 of 268 completed	809 of 809 completed	Default Group	Office 365	NIST 800-53
FedRAMP / Office 365	NonCompliant	77%	4 of 283 completed	809 of 809 completed	Default Group	Office 365	FedRAMP Moderate
Data Protection Baseline	NonCompliant	75%	5 of 280 completed	709 of 709 completed	Default Group	Microsoft 365	Data protection baseline

Disclaimer: Compliance Score is a dashboard that provides your Compliance Score and a summary of your data protection and compliance posture. It also includes recommendations to improve data protection and compliance. This is a reco



Compliance Manager (preview)

Tenant Management

Controls Info

Data entered and uploaded in Compliance Manager is accessible to your entire organization by default. For information about how to control who in your organization can access this data, see the Compliance Manager support article. Microsoft personnel do not have standing access to data that you enter or upload. Any data entered or uploaded into Compliance Manager will be stored in the United States on Microsoft Cloud Storage and replicated across Azure regions located in Southeast Asia and West Europe, which are compliant with Tier C standards of our Compliance Framework.

Notice: Please review these important changes, some of which require user action:

Compliance score calculation changes - your compliance score now includes Microsoft-managed control scores.

Set permissions for all users – all users must be assigned a provisioned role by "10/30/2019" in order to maintain access to Compliance Manager; there will no longer be a default Guest Access role. Admins may set permissions by visiting the Admin settings in Compliance Manager and assigning a role to all users. Admins are not impacted by this change; they will continue to have access.

Accept mandatory updates – important template updates are coming that will impact Compliance Score calculation and functionality. On your Templates dashboard, you will see alerts noted with a triangle icon—we strongly suggest you select Update to every alert attached to your templates to ensure your score is accurately calculated. You should also accept all updates to Assessments to ensure proper functionality.

Group: Default Group

Assessment: GDPR / Intune (EU GDPR (Intune))

Product: Intune

Certification: EU GDPR

Status: Non Compliant

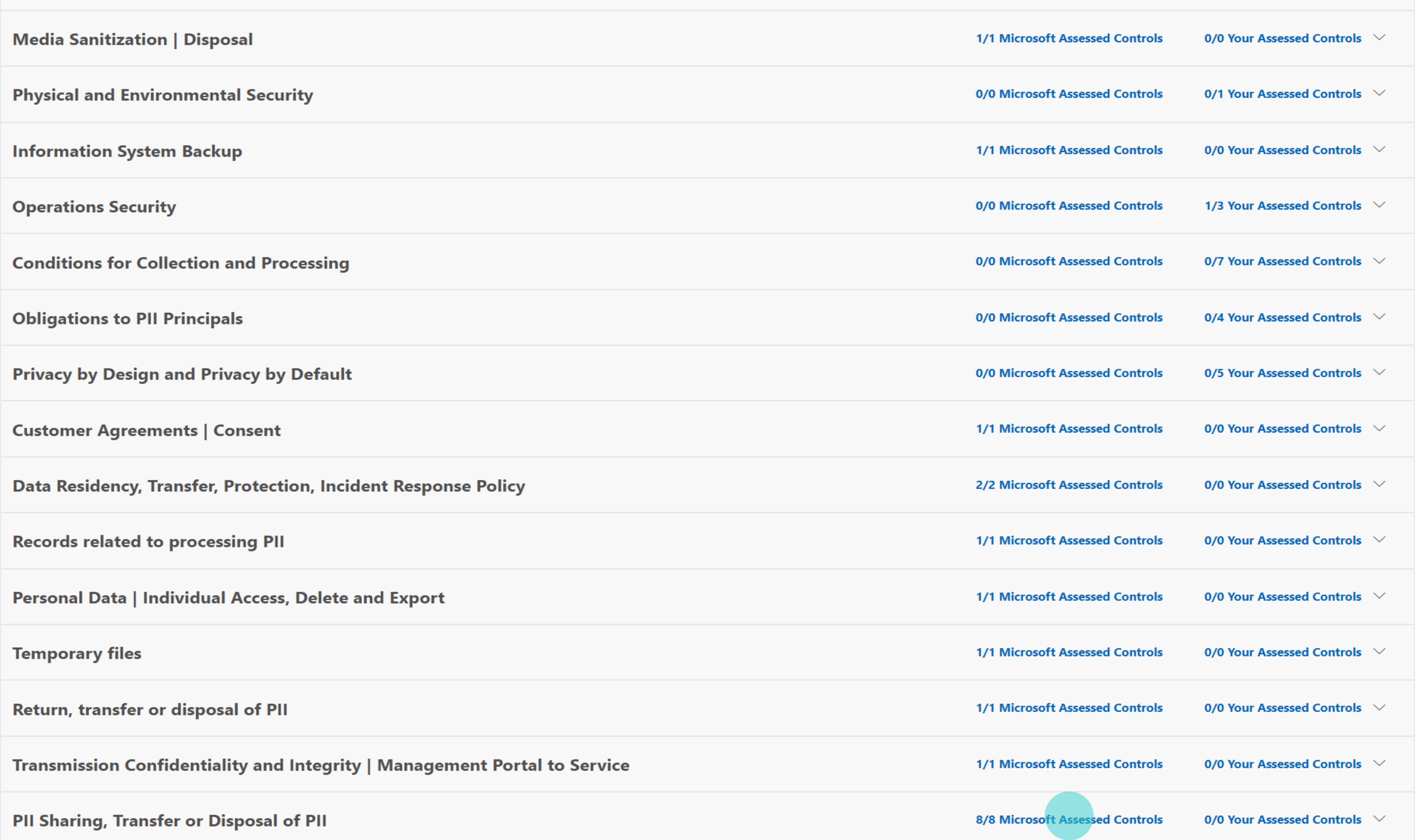
Modified: 6 days ago

Assessed Controls 1/52

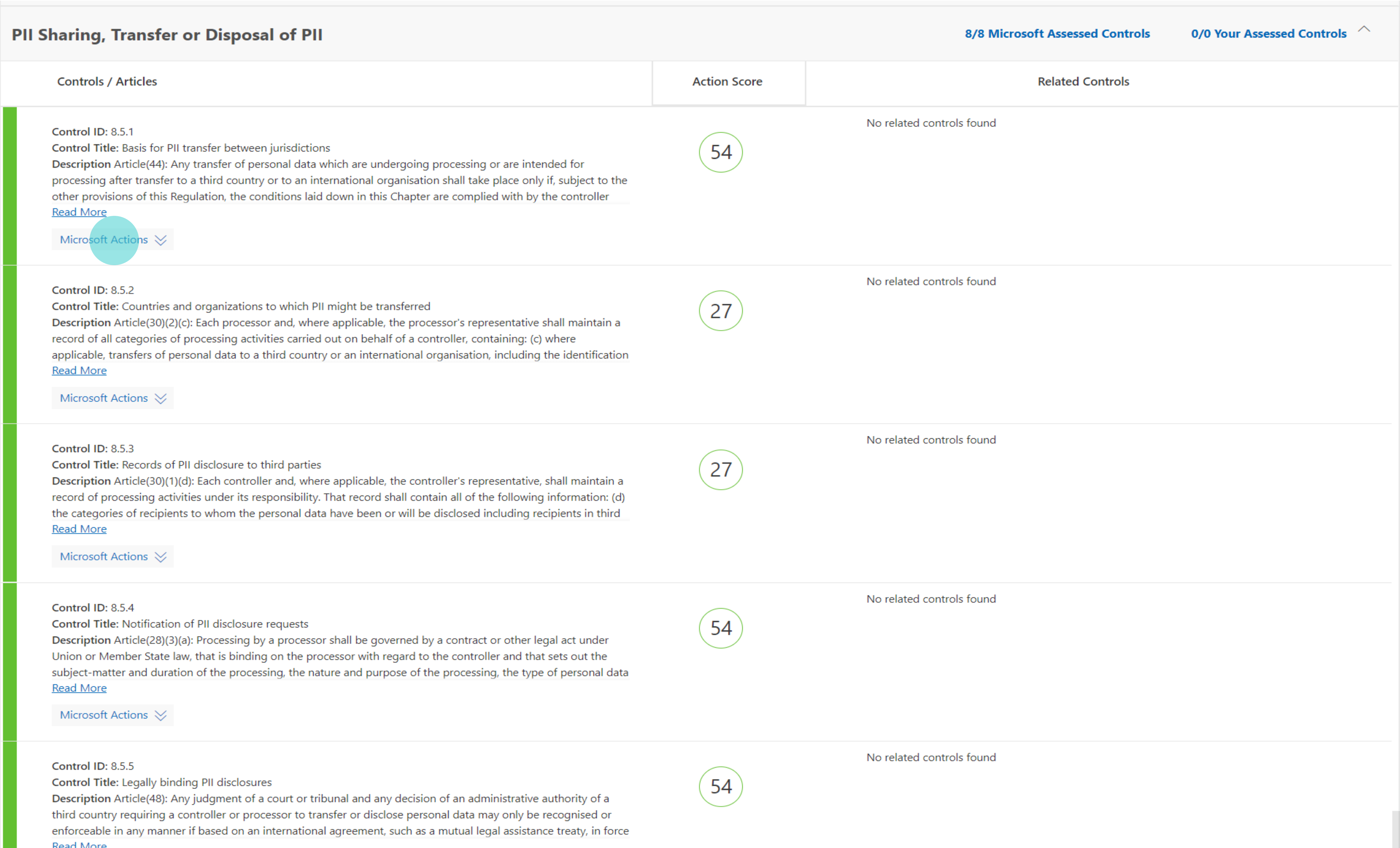
Compliance Score 45%

GDPR / Intune In Scope Services

Context of the organization	0/0 Microsoft Assessed Controls	0/4 Your Assessed Controls
Planning	0/0 Microsoft Assessed Controls	0/1 Your Assessed Controls



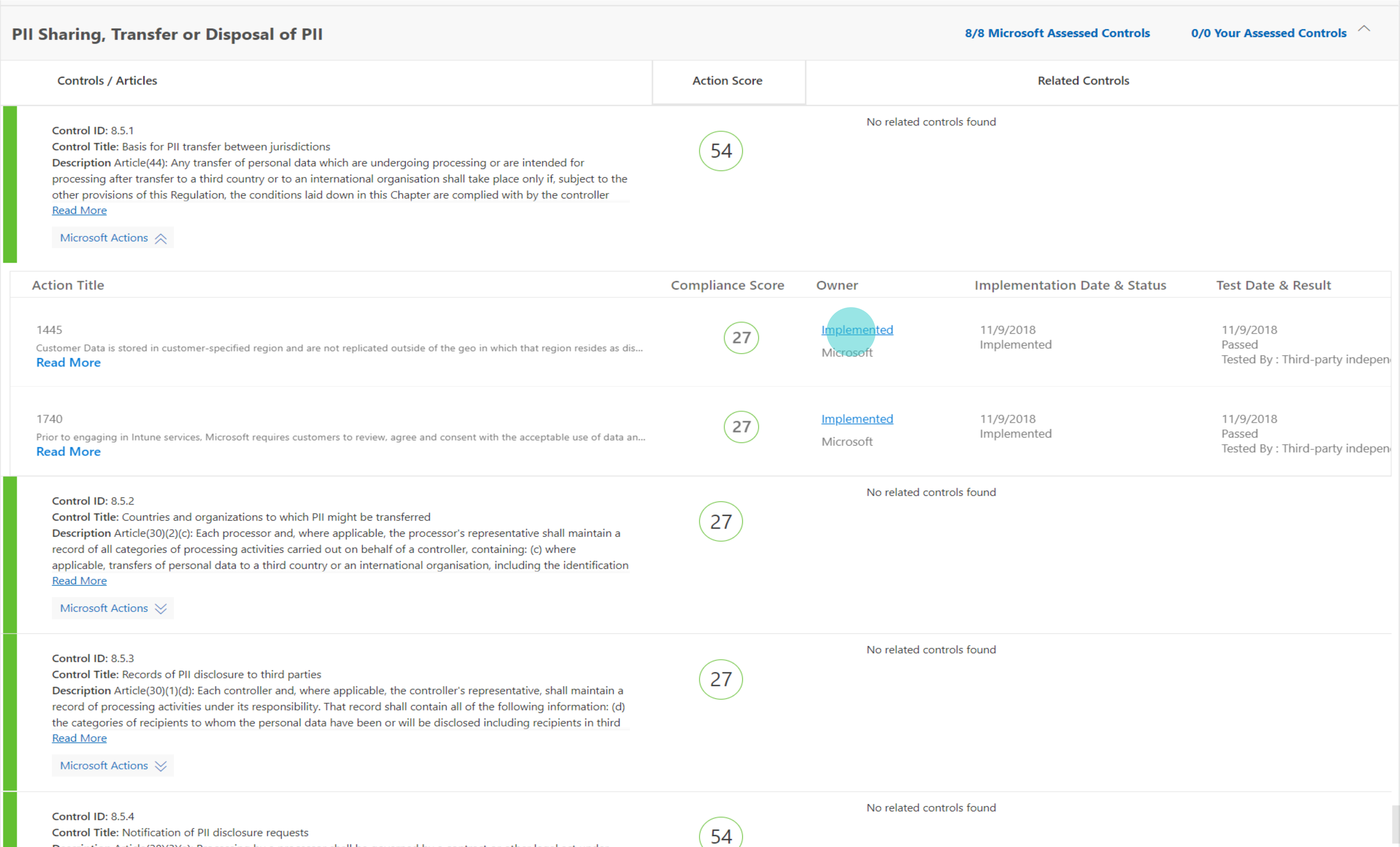
Media Sanitization | Disposal	1/1 Microsoft Assessed Controls	0/0 Your Assessed Controls
Physical and Environmental Security	0/0 Microsoft Assessed Controls	0/1 Your Assessed Controls
Information System Backup	1/1 Microsoft Assessed Controls	0/0 Your Assessed Controls
Operations Security	0/0 Microsoft Assessed Controls	1/3 Your Assessed Controls
Conditions for Collection and Processing	0/0 Microsoft Assessed Controls	0/7 Your Assessed Controls
Obligations to PII Principals	0/0 Microsoft Assessed Controls	0/4 Your Assessed Controls
Privacy by Design and Privacy by Default	0/0 Microsoft Assessed Controls	0/5 Your Assessed Controls
Customer Agreements | Consent	1/1 Microsoft Assessed Controls	0/0 Your Assessed Controls
Data Residency, Transfer, Protection, Incident Response Policy	2/2 Microsoft Assessed Controls	0/0 Your Assessed Controls
Records related to processing PII	1/1 Microsoft Assessed Controls	0/0 Your Assessed Controls
Personal Data | Individual Access, Delete and Export	1/1 Microsoft Assessed Controls	0/0 Your Assessed Controls
Temporary files	1/1 Microsoft Assessed Controls	0/0 Your Assessed Controls
Return, transfer or disposal of PII	1/1 Microsoft Assessed Controls	0/0 Your Assessed Controls
Transmission Confidentiality and Integrity | Management Portal to Service	1/1 Microsoft Assessed Controls	0/0 Your Assessed Controls
PII Sharing, Transfer or Disposal of PII	8/8 Microsoft Assessed Controls	0/0 Your Assessed Controls



PII Sharing, Transfer or Disposal of PII

8/8 Microsoft Assessed Controls 0/0 Your Assessed Controls

Controls / Articles	Action Score	Related Controls
Control ID: 8.5.1 **Control Title:** Basis for PII transfer between jurisdictions **Description** Article(44): Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller Read More Microsoft Actions	54	No related controls found
Control ID: 8.5.2 **Control Title:** Countries and organizations to which PII might be transferred **Description** Article(30)(2)(c): Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing: (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification Read More Microsoft Actions	27	No related controls found
Control ID: 8.5.3 **Control Title:** Records of PII disclosure to third parties **Description** Article(30)(1)(d): Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third Read More Microsoft Actions	27	No related controls found
Control ID: 8.5.4 **Control Title:** Notification of PII disclosure requests **Description** Article(28)(3)(a): Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data Read More Microsoft Actions	54	No related controls found
Control ID: 8.5.5 **Control Title:** Legally binding PII disclosures **Description** Article(48): Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force Read More	54	No related controls found

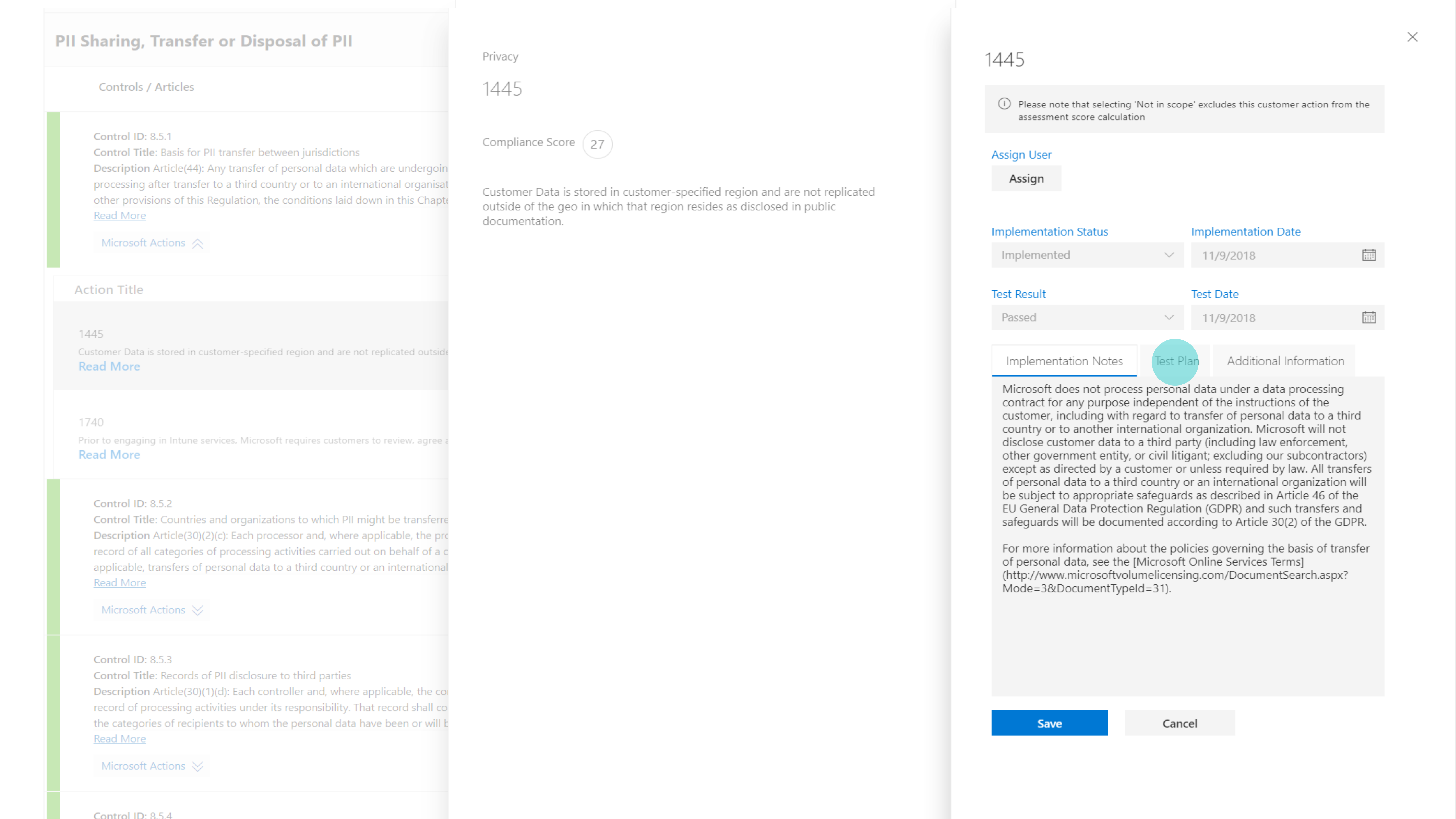


PII Sharing, Transfer or Disposal of PII

Controls / Articles	Action Score	Related Controls
Control ID: 8.5.1 **Control Title:** Basis for PII transfer between jurisdictions **Description** Article(44): Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller Read More Microsoft Actions	54	No related controls found

Action Title	Compliance Score	Owner	Implementation Date & Status	Test Date & Result
1445 Customer Data is stored in customer-specified region and are not replicated outside of the geo in which that region resides as dis... Read More	27	Implemented Microsoft	11/9/2018 Implemented	11/9/2018 Passed Tested By : Third-party indepen
1740 Prior to engaging in Intune services, Microsoft requires customers to review, agree and consent with the acceptable use of data an... Read More	27	Implemented Microsoft	11/9/2018 Implemented	11/9/2018 Passed Tested By : Third-party indepen

Controls / Articles	Action Score	Related Controls
Control ID: 8.5.2 **Control Title:** Countries and organizations to which PII might be transferred **Description** Article(30)(2)(c): Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing: (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification Read More Microsoft Actions	27	No related controls found
Control ID: 8.5.3 **Control Title:** Records of PII disclosure to third parties **Description** Article(30)(1)(d): Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third Read More Microsoft Actions	27	No related controls found
Control ID: 8.5.4 **Control Title:** Notification of PII disclosure requests	54	No related controls found



PII Sharing, Transfer or Disposal of PII

Controls / Articles

Control ID: 8.5.1
Control Title: Basis for PII transfer between jurisdictions
Description Article(44): Any transfer of personal data which are undergoin processing after transfer to a third country or to an international organisat other provisions of this Regulation, the conditions laid down in this Chapte
Read More

Action Title

1445
Customer Data is stored in customer-specified region and are not replicated outside
Read More

1740
Prior to engaging in Intune services, Microsoft requires customers to review, agree a
Read More

Control ID: 8.5.2
Control Title: Countries and organizations to which PII might be transferre
Description Article(30)(2)(c): Each processor and, where applicable, the pro record of all categories of processing activities carried out on behalf of a c applicable, transfers of personal data to a third country or an international
Read More

Control ID: 8.5.3
Control Title: Records of PII disclosure to third parties
Description Article(30)(1)(d): Each controller and, where applicable, the co record of processing activities under its responsibility. That record shall co the categories of recipients to whom the personal data have been or will b
Read More

Control ID: 8.5.4

Privacy

1445

Compliance Score 27

Customer Data is stored in customer-specified region and are not replicated outside of the geo in which that region resides as disclosed in public documentation.

1445

Please note that selecting 'Not in scope' excludes this customer action from the assessment score calculation

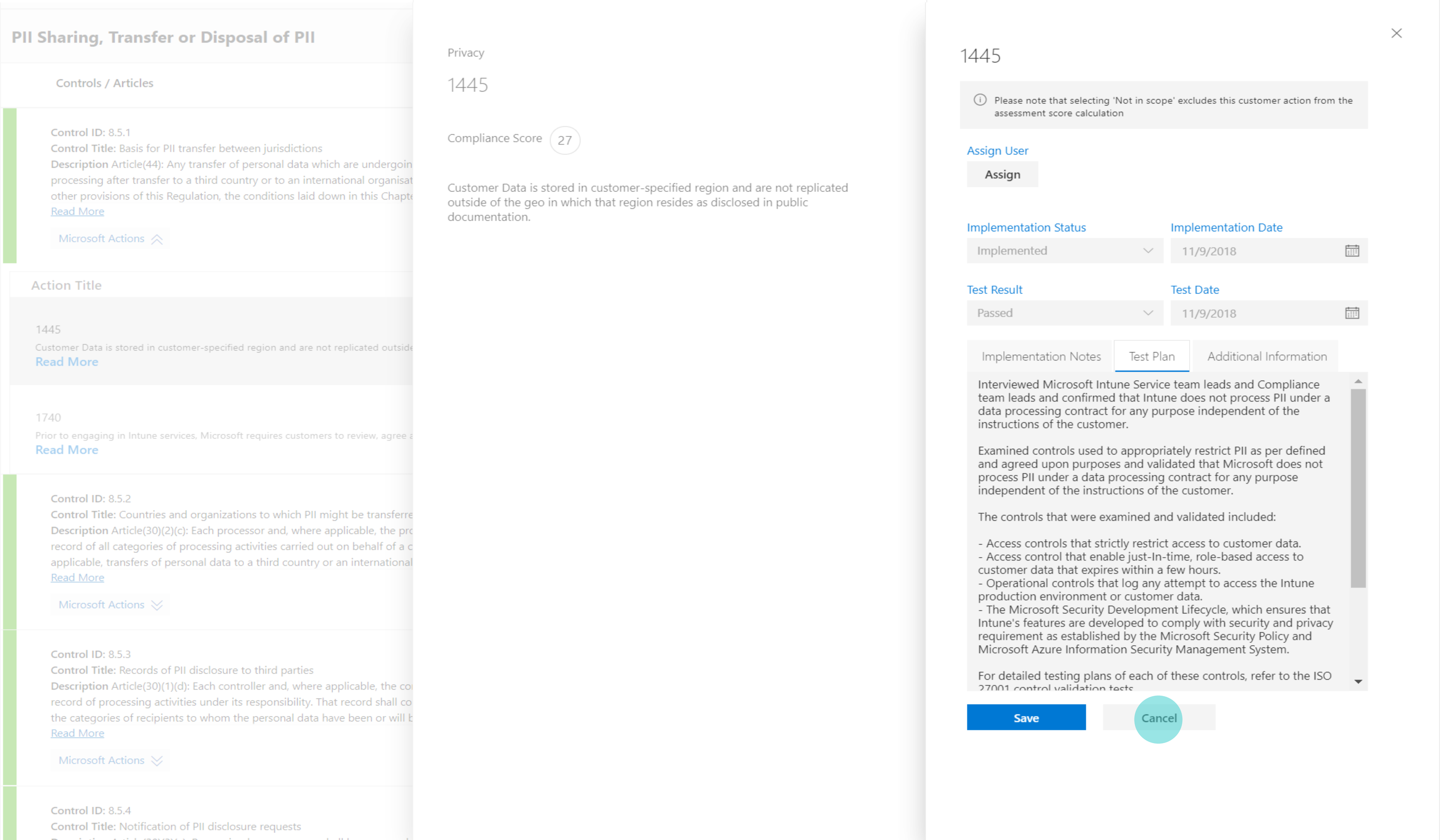
Assign User

Implementation Status: Implemented
Implementation Date: 11/9/2018

Test Result: Passed
Test Date: 11/9/2018

Microsoft does not process personal data under a data processing contract for any purpose independent of the instructions of the customer, including with regard to transfer of personal data to a third country or to another international organization. Microsoft will not disclose customer data to a third party (including law enforcement, other government entity, or civil litigant; excluding our subcontractors) except as directed by a customer or unless required by law. All transfers of personal data to a third country or an international organization will be subject to appropriate safeguards as described in Article 46 of the EU General Data Protection Regulation (GDPR) and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

For more information about the policies governing the basis of transfer of personal data, see the [Microsoft Online Services Terms](http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31).



PII Sharing, Transfer or Disposal of PII

Controls / Articles

Control ID: 8.5.1
Control Title: Basis for PII transfer between jurisdictions
Description Article(44): Any transfer of personal data which are undergoin
processing after transfer to a third country or to an international organisat
other provisions of this Regulation, the conditions laid down in this Chapte
Read More

Microsoft Actions

Action Title

1445
Customer Data is stored in customer-specified region and are not replicated outside
Read More

1740
Prior to engaging in Intune services, Microsoft requires customers to review, agree a
Read More

Control ID: 8.5.2
Control Title: Countries and organizations to which PII might be transferre
Description Article(30)(2)(c): Each processor and, where applicable, the pro
record of all categories of processing activities carried out on behalf of a c
applicable, transfers of personal data to a third country or an international
Read More

Microsoft Actions

Control ID: 8.5.3
Control Title: Records of PII disclosure to third parties
Description Article(30)(1)(d): Each controller and, where applicable, the co
record of processing activities under its responsibility. That record shall co
the categories of recipients to whom the personal data have been or will b
Read More

Microsoft Actions

Control ID: 8.5.4
Control Title: Notification of PII disclosure requests

Privacy

1445

Compliance Score 27

Customer Data is stored in customer-specified region and are not replicated outside of the geo in which that region resides as disclosed in public documentation.

1445

Please note that selecting 'Not in scope' excludes this customer action from the assessment score calculation

Assign User
Assign

Implementation Status	Implementation Date
Implemented	11/9/2018
Test Result	Test Date
Passed	11/9/2018

Implementation Notes | Test Plan | Additional Information

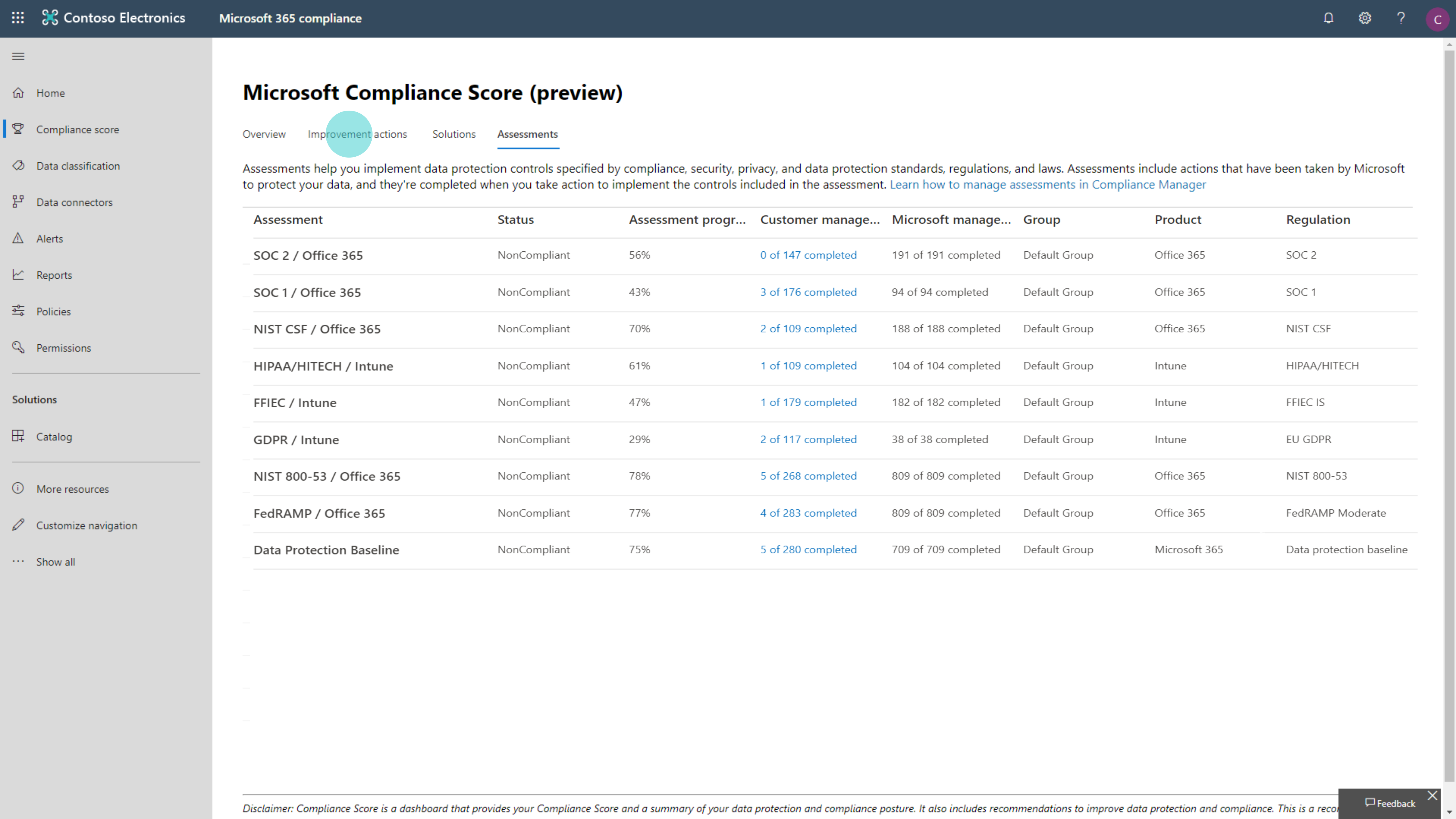
Interviewed Microsoft Intune Service team leads and Compliance team leads and confirmed that Intune does not process PII under a data processing contract for any purpose independent of the instructions of the customer.

Examined controls used to appropriately restrict PII as per defined and agreed upon purposes and validated that Microsoft does not process PII under a data processing contract for any purpose independent of the instructions of the customer.

The controls that were examined and validated included:

- Access controls that strictly restrict access to customer data.
- Access control that enable just-In-time, role-based access to customer data that expires within a few hours.
- Operational controls that log any attempt to access the Intune production environment or customer data.
- The Microsoft Security Development Lifecycle, which ensures that Intune's features are developed to comply with security and privacy requirement as established by the Microsoft Security Policy and Microsoft Azure Information Security Management System.

For detailed testing plans of each of these controls, refer to the ISO 27001 control validation tests

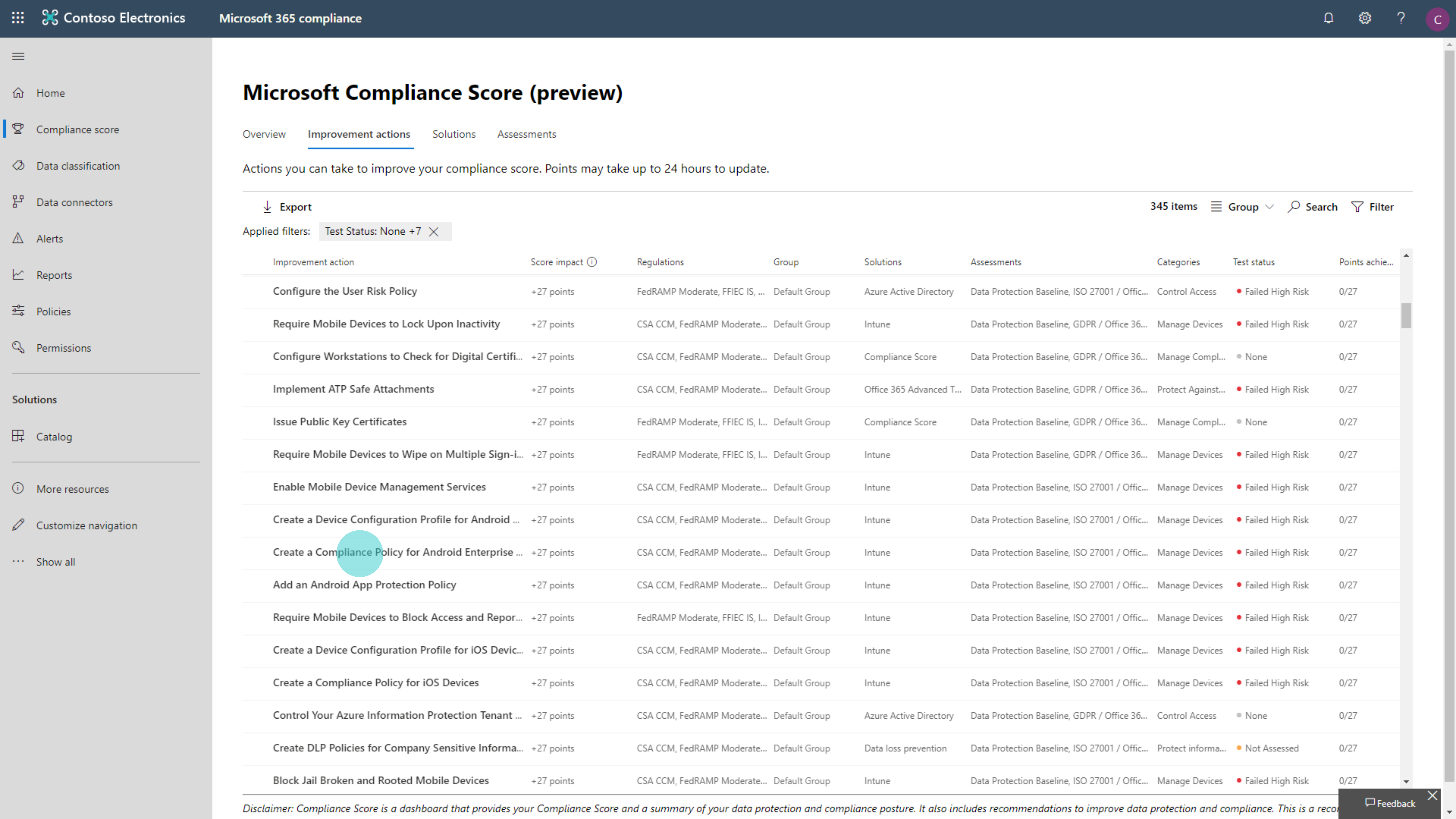


Microsoft Compliance Score (preview)

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

Assessment	Status	Assessment progr...	Customer manage...	Microsoft manage...	Group	Product	Regulation
SOC 2 / Office 365	NonCompliant	56%	0 of 147 completed	191 of 191 completed	Default Group	Office 365	SOC 2
SOC 1 / Office 365	NonCompliant	43%	3 of 176 completed	94 of 94 completed	Default Group	Office 365	SOC 1
NIST CSF / Office 365	NonCompliant	70%	2 of 109 completed	188 of 188 completed	Default Group	Office 365	NIST CSF
HIPAA/HITECH / Intune	NonCompliant	61%	1 of 109 completed	104 of 104 completed	Default Group	Intune	HIPAA/HITECH
FFIEC / Intune	NonCompliant	47%	1 of 179 completed	182 of 182 completed	Default Group	Intune	FFIEC IS
GDPR / Intune	NonCompliant	29%	2 of 117 completed	38 of 38 completed	Default Group	Intune	EU GDPR
NIST 800-53 / Office 365	NonCompliant	78%	5 of 268 completed	809 of 809 completed	Default Group	Office 365	NIST 800-53
FedRAMP / Office 365	NonCompliant	77%	4 of 283 completed	809 of 809 completed	Default Group	Office 365	FedRAMP Moderate
Data Protection Baseline	NonCompliant	75%	5 of 280 completed	709 of 709 completed	Default Group	Microsoft 365	Data protection baseline

Disclaimer: Compliance Score is a dashboard that provides your Compliance Score and a summary of your data protection and compliance posture. It also includes recommendations to improve data protection and compliance. This is a reco



Microsoft Compliance Score (preview)

Overview | Improvement actions | Solutions | Assessments

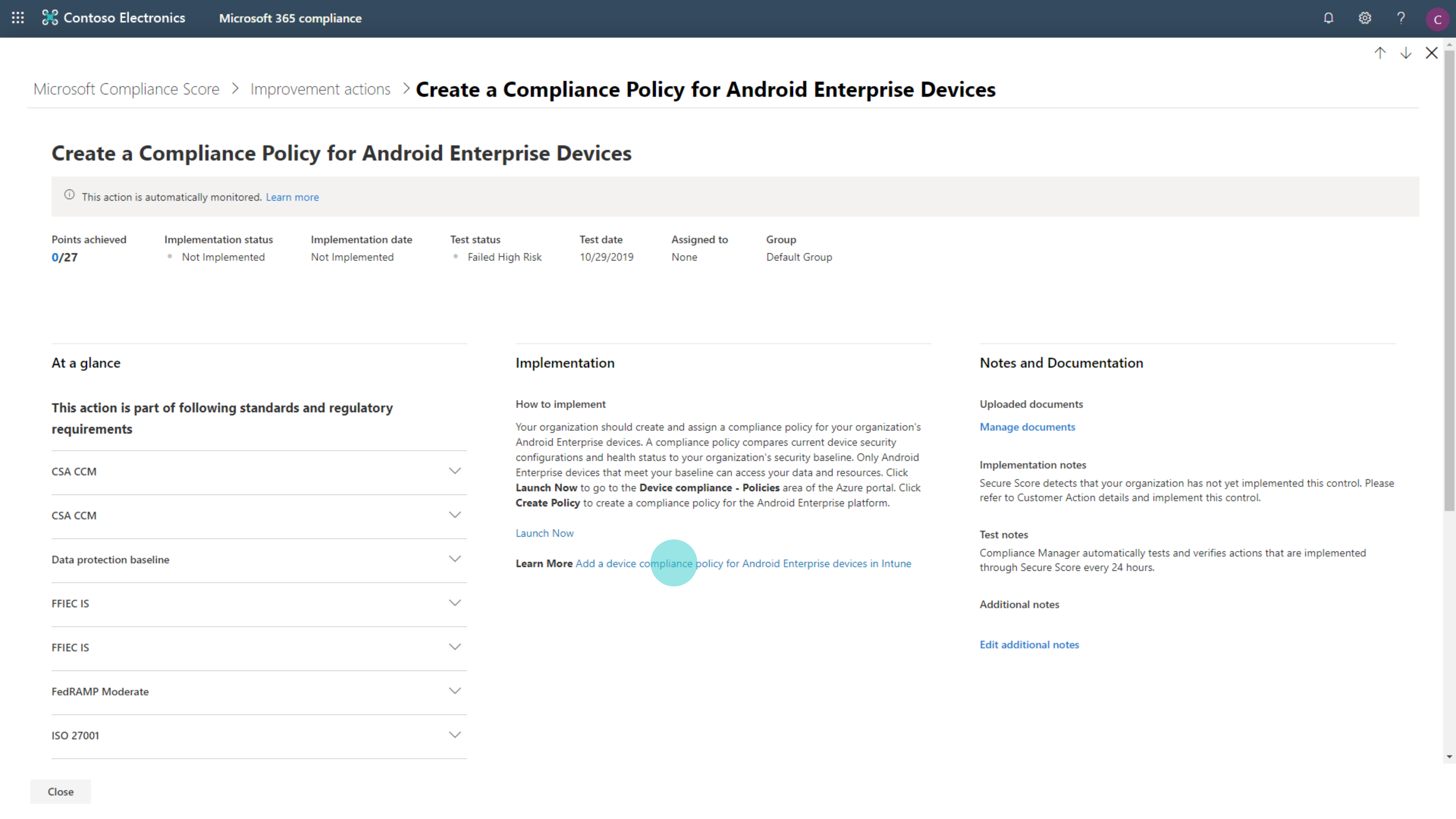
Actions you can take to improve your compliance score. Points may take up to 24 hours to update.

Export — 345 items — Group — Search — Filter

Applied filters: Test Status: None +7

Improvement action	Score impact	Regulations	Group	Solutions	Assessments	Categories	Test status	Points achie...
Configure the User Risk Policy	+27 points	FedRAMP Moderate, FFIEC IS, ...	Default Group	Azure Active Directory	Data Protection Baseline, ISO 27001 / Offic...	Control Access	● Failed High Risk	0/27
Require Mobile Devices to Lock Upon Inactivity	+27 points	CSA CCM, FedRAMP Moderate...	Default Group	Intune	Data Protection Baseline, GDPR / Office 36...	Manage Devices	● Failed High Risk	0/27
Configure Workstations to Check for Digital Certifi...	+27 points	CSA CCM, FedRAMP Moderate...	Default Group	Compliance Score	Data Protection Baseline, GDPR / Office 36...	Manage Compl...	● None	0/27
Implement ATP Safe Attachments	+27 points	CSA CCM, FedRAMP Moderate...	Default Group	Office 365 Advanced T...	Data Protection Baseline, GDPR / Office 36...	Protect Against...	● Failed High Risk	0/27
Issue Public Key Certificates	+27 points	FedRAMP Moderate, FFIEC IS, I...	Default Group	Compliance Score	Data Protection Baseline, GDPR / Office 36...	Manage Compl...	● None	0/27
Require Mobile Devices to Wipe on Multiple Sign-i...	+27 points	FedRAMP Moderate, FFIEC IS, I...	Default Group	Intune	Data Protection Baseline, GDPR / Office 36...	Manage Devices	● Failed High Risk	0/27
Enable Mobile Device Management Services	+27 points	CSA CCM, FedRAMP Moderate...	Default Group	Intune	Data Protection Baseline, ISO 27001 / Offic...	Manage Devices	● Failed High Risk	0/27
Create a Device Configuration Profile for Android ...	+27 points	CSA CCM, FedRAMP Moderate...	Default Group	Intune	Data Protection Baseline, ISO 27001 / Offic...	Manage Devices	● Failed High Risk	0/27
Create a Compliance Policy for Android Enterprise ...	+27 points	CSA CCM, FedRAMP Moderate...	Default Group	Intune	Data Protection Baseline, ISO 27001 / Offic...	Manage Devices	● Failed High Risk	0/27
Add an Android App Protection Policy	+27 points	CSA CCM, FedRAMP Moderate...	Default Group	Intune	Data Protection Baseline, ISO 27001 / Offic...	Manage Devices	● Failed High Risk	0/27
Require Mobile Devices to Block Access and Repor...	+27 points	FedRAMP Moderate, FFIEC IS, I...	Default Group	Intune	Data Protection Baseline, ISO 27001 / Offic...	Manage Devices	● Failed High Risk	0/27
Create a Device Configuration Profile for iOS Devic...	+27 points	CSA CCM, FedRAMP Moderate...	Default Group	Intune	Data Protection Baseline, ISO 27001 / Offic...	Manage Devices	● Failed High Risk	0/27
Create a Compliance Policy for iOS Devices	+27 points	CSA CCM, FedRAMP Moderate...	Default Group	Intune	Data Protection Baseline, ISO 27001 / Offic...	Manage Devices	● Failed High Risk	0/27
Control Your Azure Information Protection Tenant ...	+27 points	CSA CCM, FedRAMP Moderate...	Default Group	Azure Active Directory	Data Protection Baseline, GDPR / Office 36...	Control Access	● None	0/27
Create DLP Policies for Company Sensitive Informa...	+27 points	CSA CCM, FedRAMP Moderate...	Default Group	Data loss prevention	Data Protection Baseline, ISO 27001 / Offic...	Protect informa...	● Not Assessed	0/27
Block Jail Broken and Rooted Mobile Devices	+27 points	CSA CCM, FedRAMP Moderate...	Default Group	Intune	Data Protection Baseline, ISO 27001 / Offic...	Manage Devices	● Failed High Risk	0/27

Disclaimer: Compliance Score is a dashboard that provides your Compliance Score and a summary of your data protection and compliance posture. It also includes recommendations to improve data protection and compliance. This is a reco



Microsoft Compliance Score > Improvement actions > **Create a Compliance Policy for Android Enterprise Devices**

Create a Compliance Policy for Android Enterprise Devices

ⓘ This action is automatically monitored. Learn more

Points achieved	Implementation status	Implementation date	Test status	Test date	Assigned to	Group
0/27	● Not Implemented	Not Implemented	● Failed High Risk	10/29/2019	None	Default Group

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- Data protection baseline
- FFIEC IS
- FFIEC IS
- FedRAMP Moderate
- ISO 27001

Implementation

How to implement

Your organization should create and assign a compliance policy for your organization's Android Enterprise devices. A compliance policy compares current device security configurations and health status to your organization's security baseline. Only Android Enterprise devices that meet your baseline can access your data and resources. Click **Launch Now** to go to the **Device compliance - Policies** area of the Azure portal. Click **Create Policy** to create a compliance policy for the Android Enterprise platform.

Launch Now

Learn More Add a device compliance policy for Android Enterprise devices in Intune

Notes and Documentation

Uploaded documents

Manage documents

Implementation notes

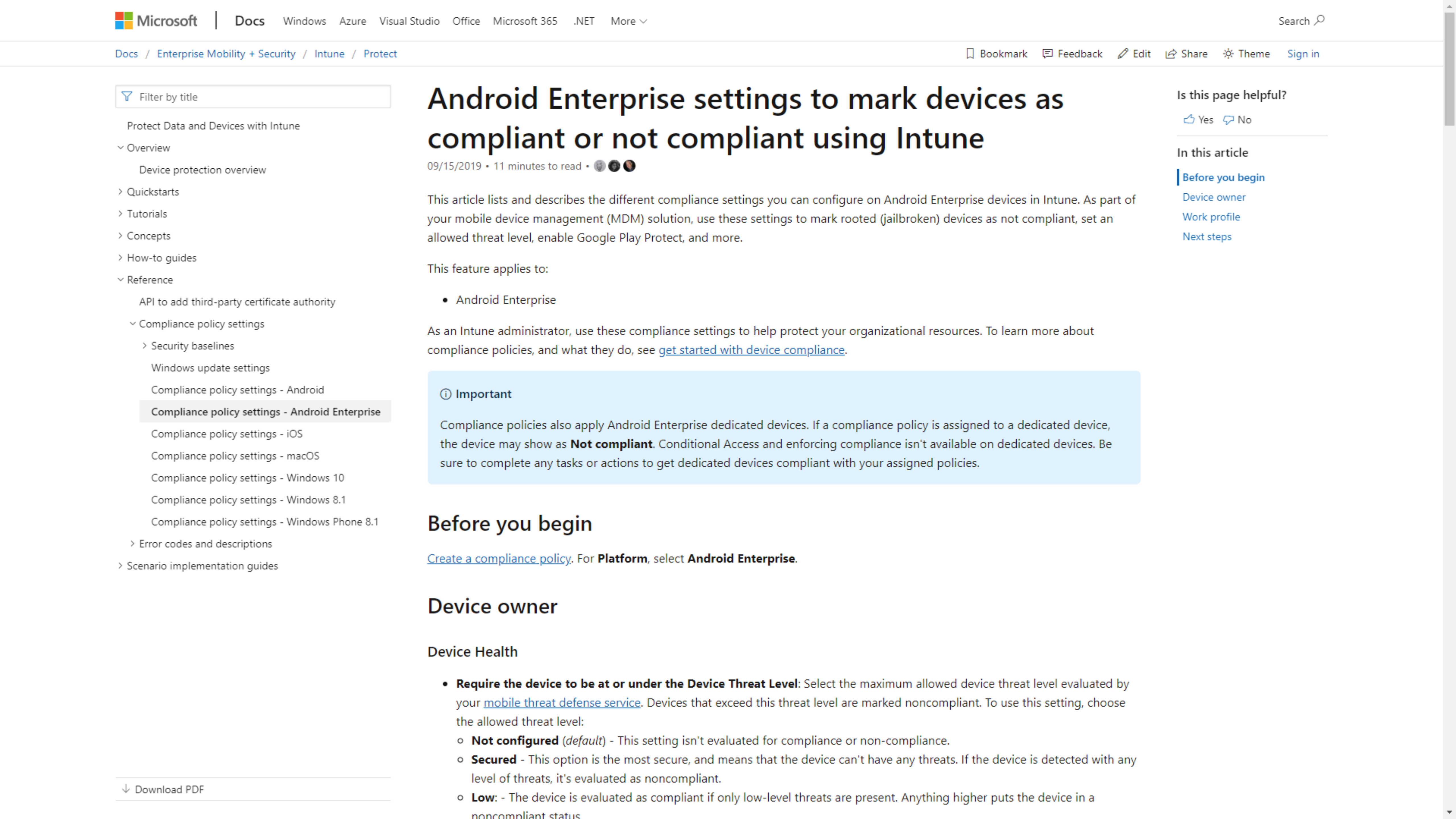
Secure Score detects that your organization has not yet implemented this control. Please refer to Customer Action details and implement this control.

Test notes

Compliance Manager automatically tests and verifies actions that are implemented through Secure Score every 24 hours.

Additional notes

Edit additional notes



Filter by title

Protect Data and Devices with Intune
Overview
Device protection overview
Quickstarts
Tutorials
Concepts
How-to guides
Reference
API to add third-party certificate authority
Compliance policy settings
Security baselines
Windows update settings
Compliance policy settings - Android
Compliance policy settings - Android Enterprise
Compliance policy settings - iOS
Compliance policy settings - macOS
Compliance policy settings - Windows 10
Compliance policy settings - Windows 8.1
Compliance policy settings - Windows Phone 8.1
Error codes and descriptions
Scenario implementation guides

Download PDF

Android Enterprise settings to mark devices as compliant or not compliant using Intune

09/15/2019 • 11 minutes to read •

This article lists and describes the different compliance settings you can configure on Android Enterprise devices in Intune. As part of your mobile device management (MDM) solution, use these settings to mark rooted (jailbroken) devices as not compliant, set an allowed threat level, enable Google Play Protect, and more.

This feature applies to:

- Android Enterprise

As an Intune administrator, use these compliance settings to help protect your organizational resources. To learn more about compliance policies, and what they do, see get started with device compliance.

> ⓘ Important
>
> Compliance policies also apply Android Enterprise dedicated devices. If a compliance policy is assigned to a dedicated device, the device may show as **Not compliant**. Conditional Access and enforcing compliance isn't available on dedicated devices. Be sure to complete any tasks or actions to get dedicated devices compliant with your assigned policies.

Before you begin

Create a compliance policy. For **Platform**, select **Android Enterprise**.

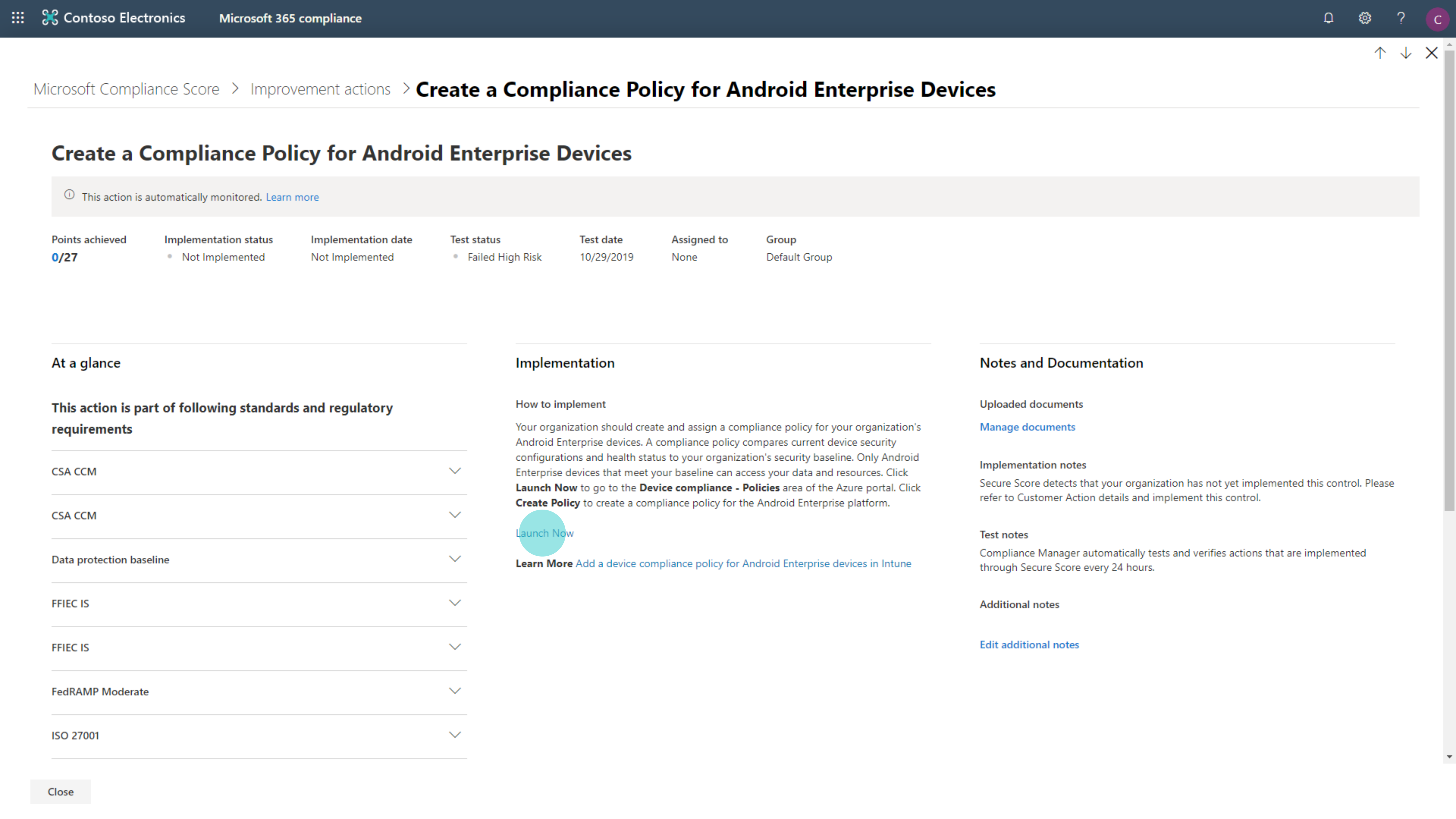
Device owner

Device Health

- **Require the device to be at or under the Device Threat Level**: Select the maximum allowed device threat level evaluated by your mobile threat defense service. Devices that exceed this threat level are marked noncompliant. To use this setting, choose the allowed threat level:
  - **Not configured** (*default*) - This setting isn't evaluated for compliance or non-compliance.
  - **Secured** - This option is the most secure, and means that the device can't have any threats. If the device is detected with any level of threats, it's evaluated as noncompliant.
  - **Low**: - The device is evaluated as compliant if only low-level threats are present. Anything higher puts the device in a noncompliant status.

Is this page helpful?
Yes No

In this article
Before you begin
Device owner
Work profile
Next steps



Microsoft Compliance Score > Improvement actions > **Create a Compliance Policy for Android Enterprise Devices**

Create a Compliance Policy for Android Enterprise Devices

ⓘ This action is automatically monitored. Learn more

Points achieved	Implementation status	Implementation date	Test status	Test date	Assigned to	Group
0/27	● Not Implemented	Not Implemented	● Failed High Risk	10/29/2019	None	Default Group

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- Data protection baseline
- FFIEC IS
- FFIEC IS
- FedRAMP Moderate
- ISO 27001

Implementation

How to implement

Your organization should create and assign a compliance policy for your organization's Android Enterprise devices. A compliance policy compares current device security configurations and health status to your organization's security baseline. Only Android Enterprise devices that meet your baseline can access your data and resources. Click **Launch Now** to go to the **Device compliance - Policies** area of the Azure portal. Click **Create Policy** to create a compliance policy for the Android Enterprise platform.

Launch Now

Learn More Add a device compliance policy for Android Enterprise devices in Intune

Notes and Documentation

Uploaded documents

Manage documents

Implementation notes

Secure Score detects that your organization has not yet implemented this control. Please refer to Customer Action details and implement this control.

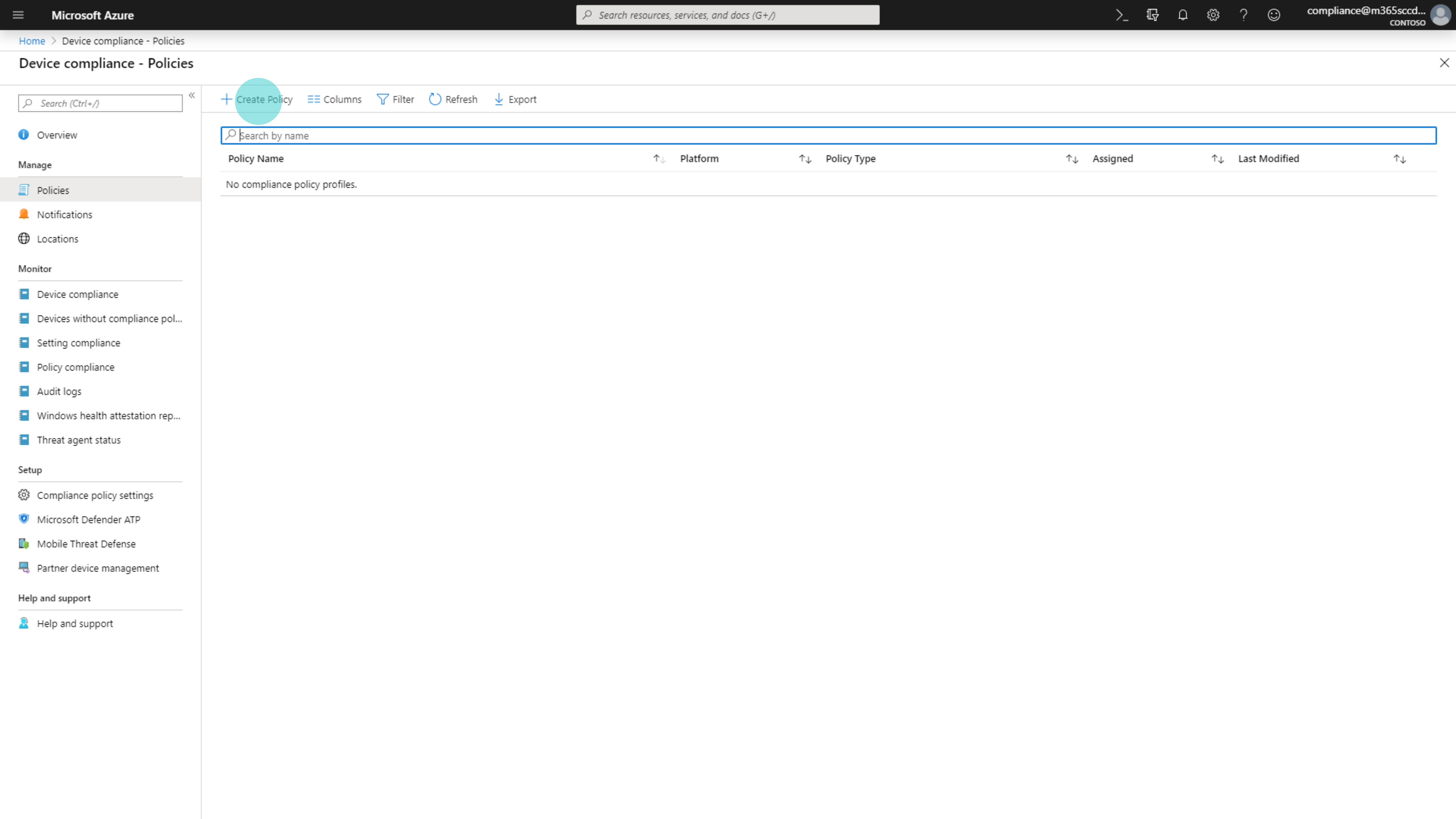
Test notes

Compliance Manager automatically tests and verifies actions that are implemented through Secure Score every 24 hours.

Additional notes

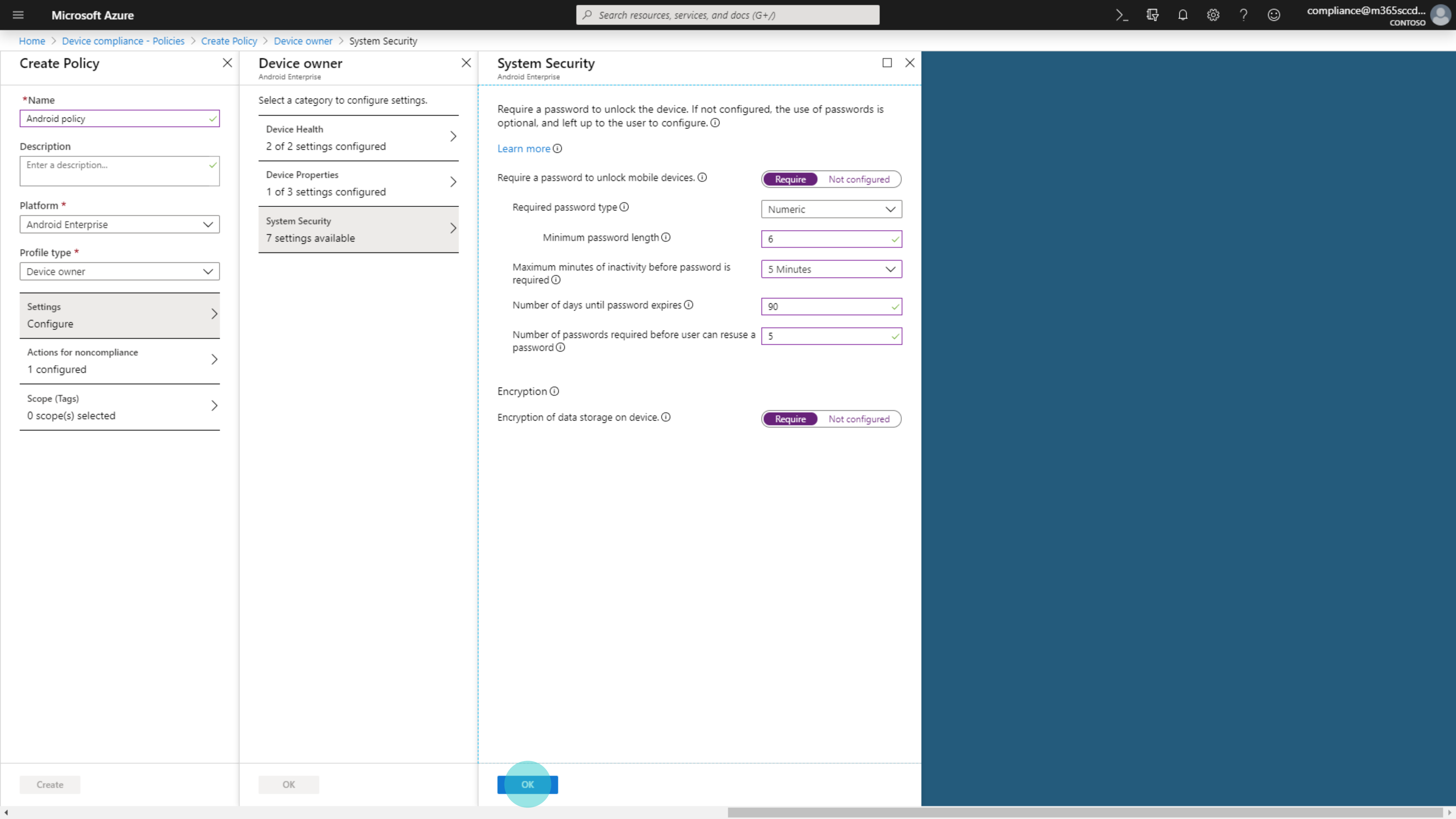
Edit additional notes

Close



Device compliance - Policies

Policy Name	Platform	Policy Type	Assigned	Last Modified
No compliance policy profiles.				



Home > Device compliance - Policies > Create Policy > Device owner > System Security

Create Policy

*Name: Android policy

Description: Enter a description...

Platform *: Android Enterprise

Profile type *: Device owner

Settings
Configure

Actions for noncompliance
1 configured

Scope (Tags)
0 scope(s) selected

Device owner

Android Enterprise

Select a category to configure settings.

Device Health
2 of 2 settings configured

Device Properties
1 of 3 settings configured

System Security
7 settings available

System Security

Android Enterprise

Require a password to unlock the device. If not configured, the use of passwords is optional, and left up to the user to configure.

Learn more

Require a password to unlock mobile devices.: [✓ Require] Not configured

Required password type: Numeric

Minimum password length: 6

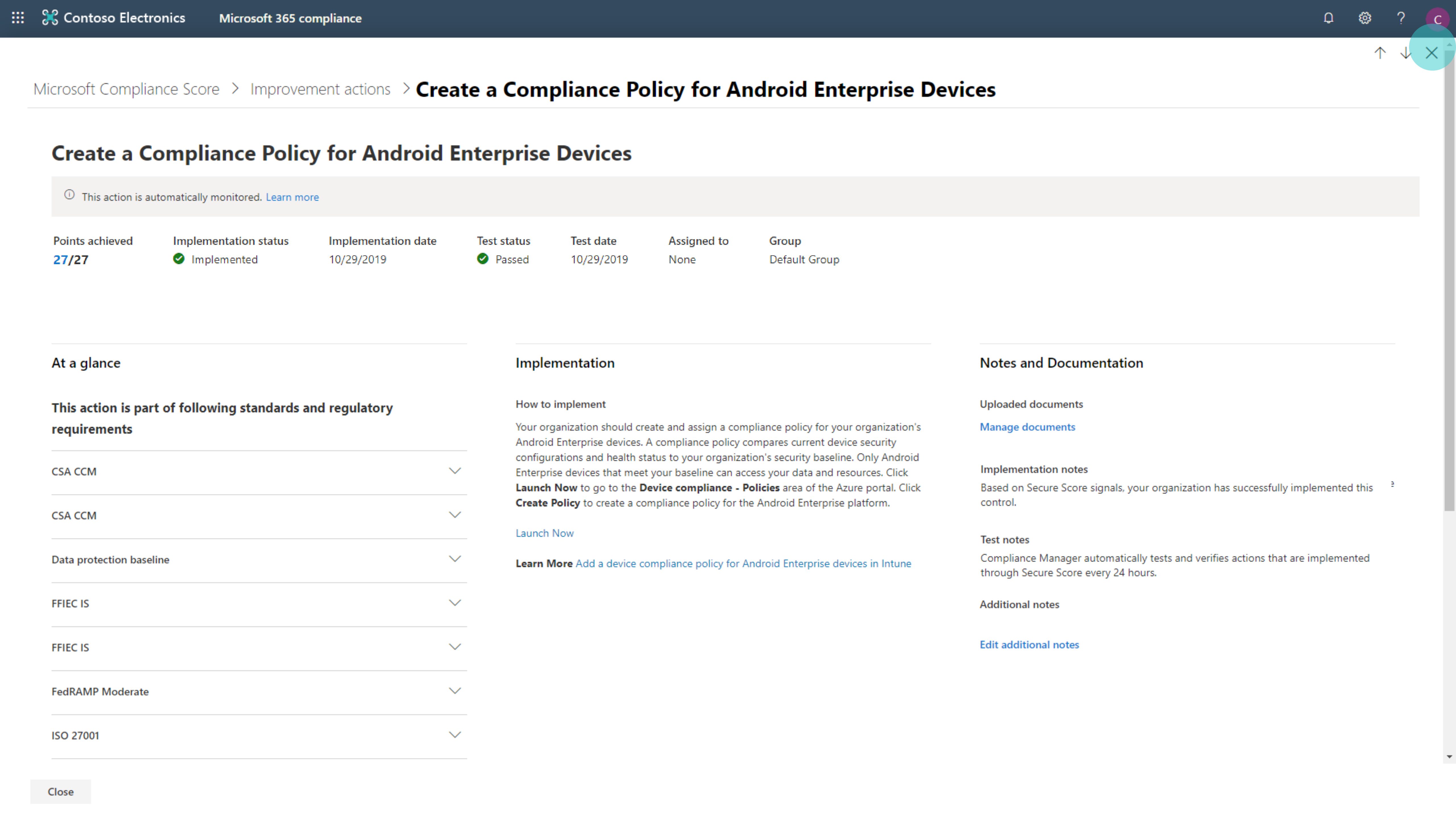
Maximum minutes of inactivity before password is required: 5 Minutes

Number of days until password expires: 90

Number of passwords required before user can resuse a password: 5

Encryption

Encryption of data storage on device.: [✓ Require] Not configured



Microsoft Compliance Score > Improvement actions > **Create a Compliance Policy for Android Enterprise Devices**

Create a Compliance Policy for Android Enterprise Devices

ⓘ This action is automatically monitored. Learn more

Points achieved	Implementation status	Implementation date	Test status	Test date	Assigned to	Group
27/27	✓ Implemented	10/29/2019	✓ Passed	10/29/2019	None	Default Group

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- Data protection baseline
- FFIEC IS
- FFIEC IS
- FedRAMP Moderate
- ISO 27001

Implementation

How to implement

Your organization should create and assign a compliance policy for your organization's Android Enterprise devices. A compliance policy compares current device security configurations and health status to your organization's security baseline. Only Android Enterprise devices that meet your baseline can access your data and resources. Click **Launch Now** to go to the **Device compliance - Policies** area of the Azure portal. Click **Create Policy** to create a compliance policy for the Android Enterprise platform.

Launch Now

Learn More Add a device compliance policy for Android Enterprise devices in Intune

Notes and Documentation

Uploaded documents

Manage documents

Implementation notes

Based on Secure Score signals, your organization has successfully implemented this control.

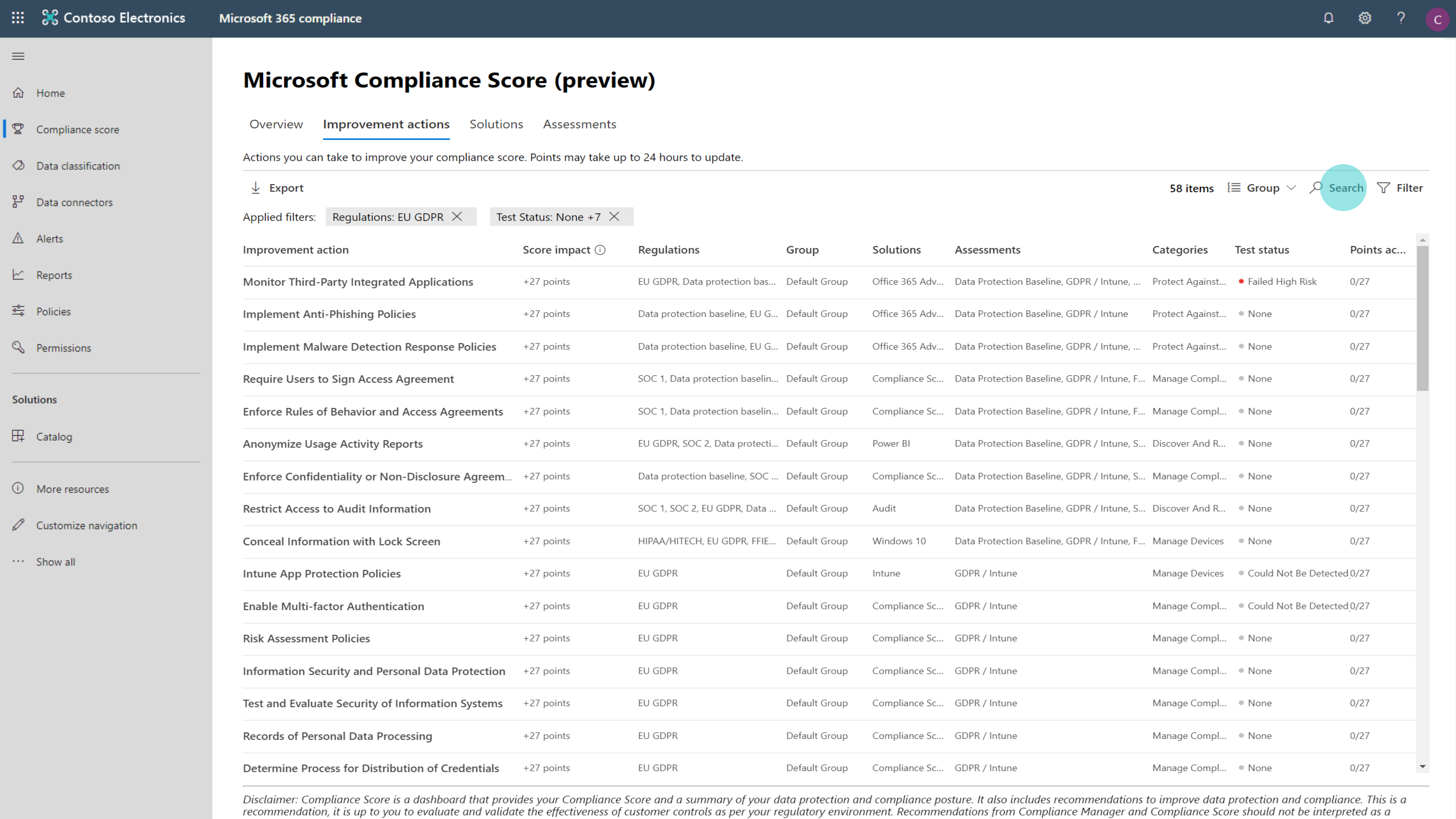
Test notes

Compliance Manager automatically tests and verifies actions that are implemented through Secure Score every 24 hours.

Additional notes

Edit additional notes

Close



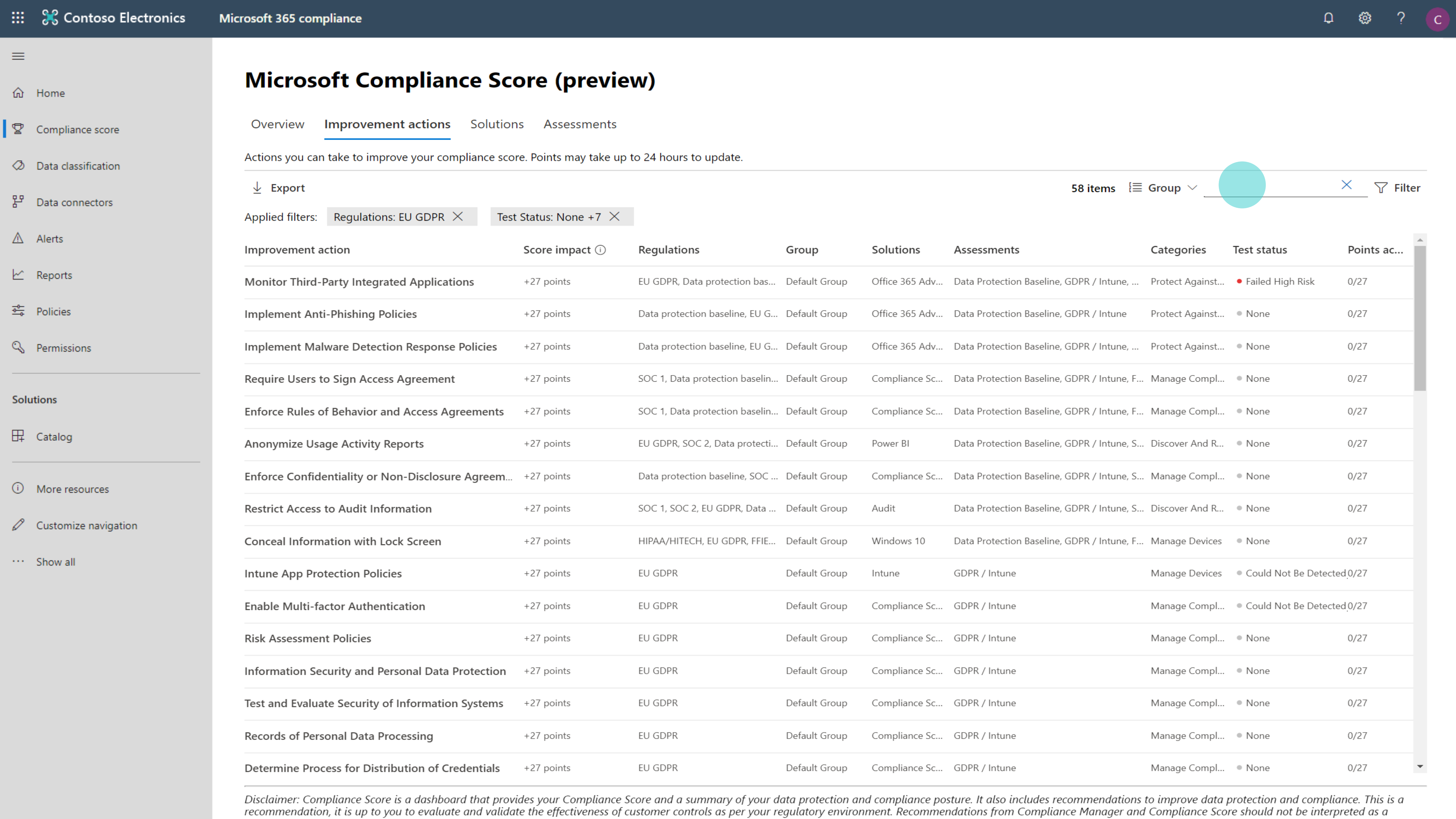
Microsoft Compliance Score (preview)

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

Applied filters: Regulations: EU GDPR ✕ Test Status: None +7 ✕

Improvement action	Score impact ⓘ	Regulations	Group	Solutions	Assessments	Categories	Test status	Points ac...
Monitor Third-Party Integrated Applications	+27 points	EU GDPR, Data protection bas...	Default Group	Office 365 Adv...	Data Protection Baseline, GDPR / Intune, ...	Protect Against...	● Failed High Risk	0/27
Implement Anti-Phishing Policies	+27 points	Data protection baseline, EU G...	Default Group	Office 365 Adv...	Data Protection Baseline, GDPR / Intune	Protect Against...	● None	0/27
Implement Malware Detection Response Policies	+27 points	Data protection baseline, EU G...	Default Group	Office 365 Adv...	Data Protection Baseline, GDPR / Intune, ...	Protect Against...	● None	0/27
Require Users to Sign Access Agreement	+27 points	SOC 1, Data protection baselin...	Default Group	Compliance Sc...	Data Protection Baseline, GDPR / Intune, F...	Manage Compl...	● None	0/27
Enforce Rules of Behavior and Access Agreements	+27 points	SOC 1, Data protection baselin...	Default Group	Compliance Sc...	Data Protection Baseline, GDPR / Intune, F...	Manage Compl...	● None	0/27
Anonymize Usage Activity Reports	+27 points	EU GDPR, SOC 2, Data protecti...	Default Group	Power BI	Data Protection Baseline, GDPR / Intune, S...	Discover And R...	● None	0/27
Enforce Confidentiality or Non-Disclosure Agreem...	+27 points	Data protection baseline, SOC ...	Default Group	Compliance Sc...	Data Protection Baseline, GDPR / Intune, S...	Manage Compl...	● None	0/27
Restrict Access to Audit Information	+27 points	SOC 1, SOC 2, EU GDPR, Data ...	Default Group	Audit	Data Protection Baseline, GDPR / Intune, S...	Discover And R...	● None	0/27
Conceal Information with Lock Screen	+27 points	HIPAA/HITECH, EU GDPR, FFIE...	Default Group	Windows 10	Data Protection Baseline, GDPR / Intune, F...	Manage Devices	● None	0/27
Intune App Protection Policies	+27 points	EU GDPR	Default Group	Intune	GDPR / Intune	Manage Devices	● Could Not Be Detected	0/27
Enable Multi-factor Authentication	+27 points	EU GDPR	Default Group	Compliance Sc...	GDPR / Intune	Manage Compl...	● Could Not Be Detected	0/27
Risk Assessment Policies	+27 points	EU GDPR	Default Group	Compliance Sc...	GDPR / Intune	Manage Compl...	● None	0/27
Information Security and Personal Data Protection	+27 points	EU GDPR	Default Group	Compliance Sc...	GDPR / Intune	Manage Compl...	● None	0/27
Test and Evaluate Security of Information Systems	+27 points	EU GDPR	Default Group	Compliance Sc...	GDPR / Intune	Manage Compl...	● None	0/27
Records of Personal Data Processing	+27 points	EU GDPR	Default Group	Compliance Sc...	GDPR / Intune	Manage Compl...	● None	0/27
Determine Process for Distribution of Credentials	+27 points	EU GDPR	Default Group	Compliance Sc...	GDPR / Intune	Manage Compl...	● None	0/27

Disclaimer: Compliance Score is a dashboard that provides your Compliance Score and a summary of your data protection and compliance posture. It also includes recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a



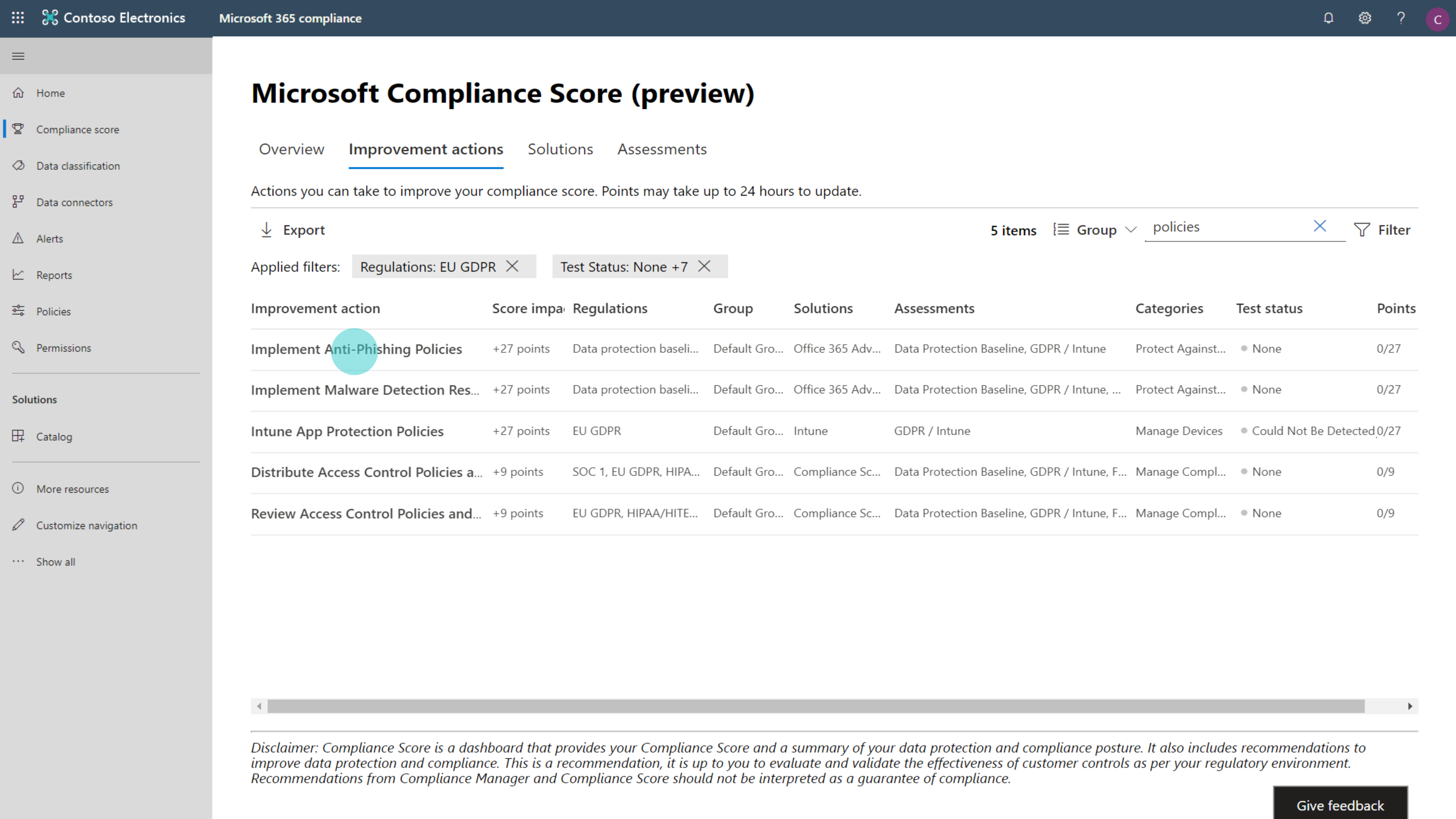
Microsoft Compliance Score (preview)

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

Applied filters: Regulations: EU GDPR ✕ Test Status: None +7 ✕

Improvement action	Score impact	Regulations	Group	Solutions	Assessments	Categories	Test status	Points ac...
Monitor Third-Party Integrated Applications	+27 points	EU GDPR, Data protection bas...	Default Group	Office 365 Adv...	Data Protection Baseline, GDPR / Intune, ...	Protect Against...	● Failed High Risk	0/27
Implement Anti-Phishing Policies	+27 points	Data protection baseline, EU G...	Default Group	Office 365 Adv...	Data Protection Baseline, GDPR / Intune	Protect Against...	● None	0/27
Implement Malware Detection Response Policies	+27 points	Data protection baseline, EU G...	Default Group	Office 365 Adv...	Data Protection Baseline, GDPR / Intune, ...	Protect Against...	● None	0/27
Require Users to Sign Access Agreement	+27 points	SOC 1, Data protection baselin...	Default Group	Compliance Sc...	Data Protection Baseline, GDPR / Intune, F...	Manage Compl...	● None	0/27
Enforce Rules of Behavior and Access Agreements	+27 points	SOC 1, Data protection baselin...	Default Group	Compliance Sc...	Data Protection Baseline, GDPR / Intune, F...	Manage Compl...	● None	0/27
Anonymize Usage Activity Reports	+27 points	EU GDPR, SOC 2, Data protecti...	Default Group	Power BI	Data Protection Baseline, GDPR / Intune, S...	Discover And R...	● None	0/27
Enforce Confidentiality or Non-Disclosure Agreem...	+27 points	Data protection baseline, SOC ...	Default Group	Compliance Sc...	Data Protection Baseline, GDPR / Intune, S...	Manage Compl...	● None	0/27
Restrict Access to Audit Information	+27 points	SOC 1, SOC 2, EU GDPR, Data ...	Default Group	Audit	Data Protection Baseline, GDPR / Intune, S...	Discover And R...	● None	0/27
Conceal Information with Lock Screen	+27 points	HIPAA/HITECH, EU GDPR, FFIE...	Default Group	Windows 10	Data Protection Baseline, GDPR / Intune, F...	Manage Devices	● None	0/27
Intune App Protection Policies	+27 points	EU GDPR	Default Group	Intune	GDPR / Intune	Manage Devices	● Could Not Be Detected	0/27
Enable Multi-factor Authentication	+27 points	EU GDPR	Default Group	Compliance Sc...	GDPR / Intune	Manage Compl...	● Could Not Be Detected	0/27
Risk Assessment Policies	+27 points	EU GDPR	Default Group	Compliance Sc...	GDPR / Intune	Manage Compl...	● None	0/27
Information Security and Personal Data Protection	+27 points	EU GDPR	Default Group	Compliance Sc...	GDPR / Intune	Manage Compl...	● None	0/27
Test and Evaluate Security of Information Systems	+27 points	EU GDPR	Default Group	Compliance Sc...	GDPR / Intune	Manage Compl...	● None	0/27
Records of Personal Data Processing	+27 points	EU GDPR	Default Group	Compliance Sc...	GDPR / Intune	Manage Compl...	● None	0/27
Determine Process for Distribution of Credentials	+27 points	EU GDPR	Default Group	Compliance Sc...	GDPR / Intune	Manage Compl...	● None	0/27

Disclaimer: Compliance Score is a dashboard that provides your Compliance Score and a summary of your data protection and compliance posture. It also includes recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a



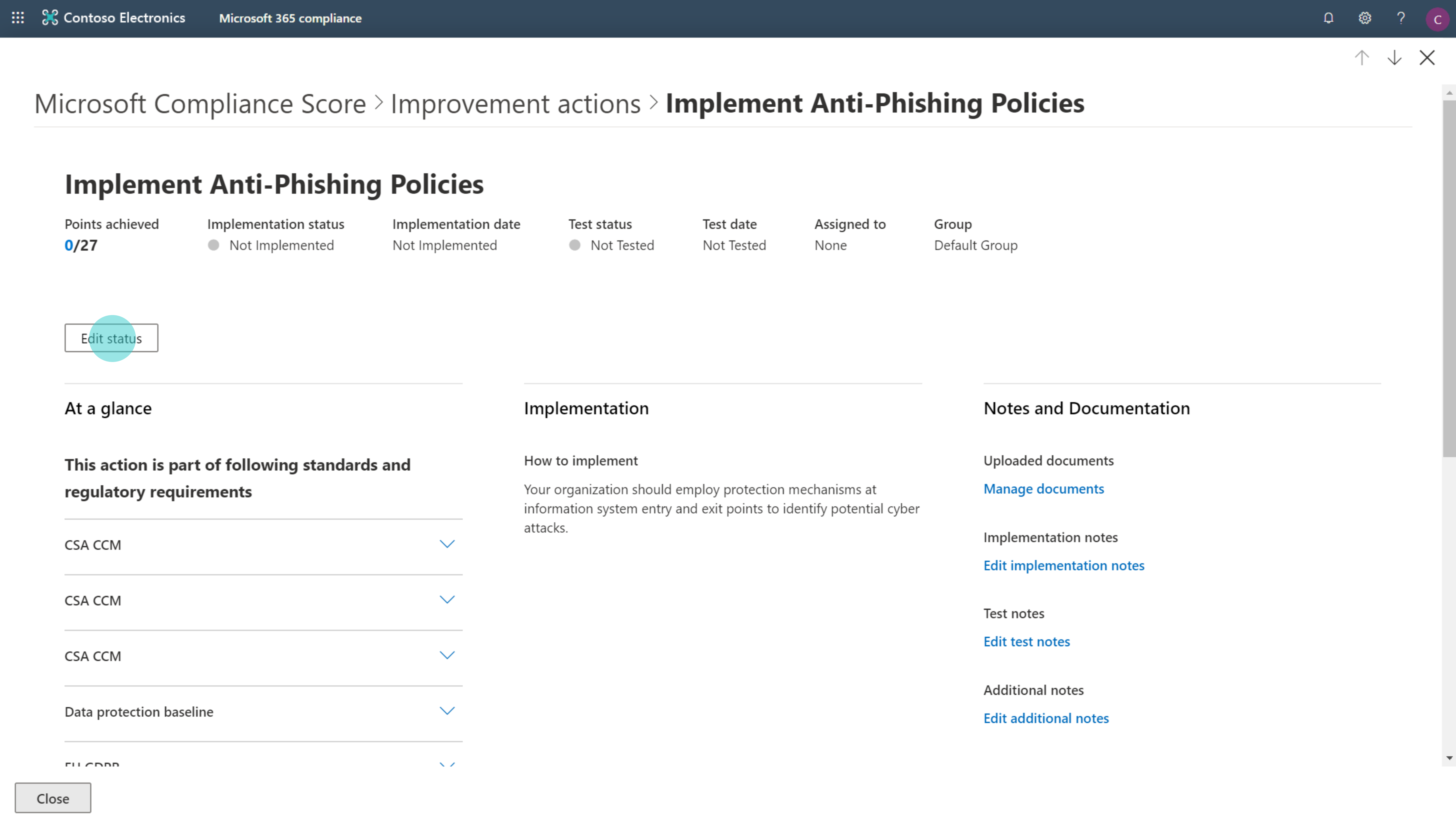
Microsoft Compliance Score (preview)

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

Applied filters: Regulations: EU GDPR ✕ Test Status: None +7 ✕

Improvement action	Score impa	Regulations	Group	Solutions	Assessments	Categories	Test status	Points
Implement Anti-Phishing Policies	+27 points	Data protection baseli...	Default Gro...	Office 365 Adv...	Data Protection Baseline, GDPR / Intune	Protect Against...	● None	0/27
Implement Malware Detection Res...	+27 points	Data protection baseli...	Default Gro...	Office 365 Adv...	Data Protection Baseline, GDPR / Intune, ...	Protect Against...	● None	0/27
Intune App Protection Policies	+27 points	EU GDPR	Default Gro...	Intune	GDPR / Intune	Manage Devices	● Could Not Be Detected	0/27
Distribute Access Control Policies a...	+9 points	SOC 1, EU GDPR, HIPA...	Default Gro...	Compliance Sc...	Data Protection Baseline, GDPR / Intune, F...	Manage Compl...	● None	0/9
Review Access Control Policies and...	+9 points	EU GDPR, HIPAA/HITE...	Default Gro...	Compliance Sc...	Data Protection Baseline, GDPR / Intune, F...	Manage Compl...	● None	0/9

Disclaimer: Compliance Score is a dashboard that provides your Compliance Score and a summary of your data protection and compliance posture. It also includes recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a guarantee of compliance.



Microsoft Compliance Score > Improvement actions > **Implement Anti-Phishing Policies**

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date	Assigned to	Group
0/27	● Not Implemented	Not Implemented	● Not Tested	Not Tested	None	Default Group

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline
- EU GDPR

Implementation

How to implement

Your organization should employ protection mechanisms at information system entry and exit points to identify potential cyber attacks.

Notes and Documentation

Uploaded documents

Manage documents

Implementation notes

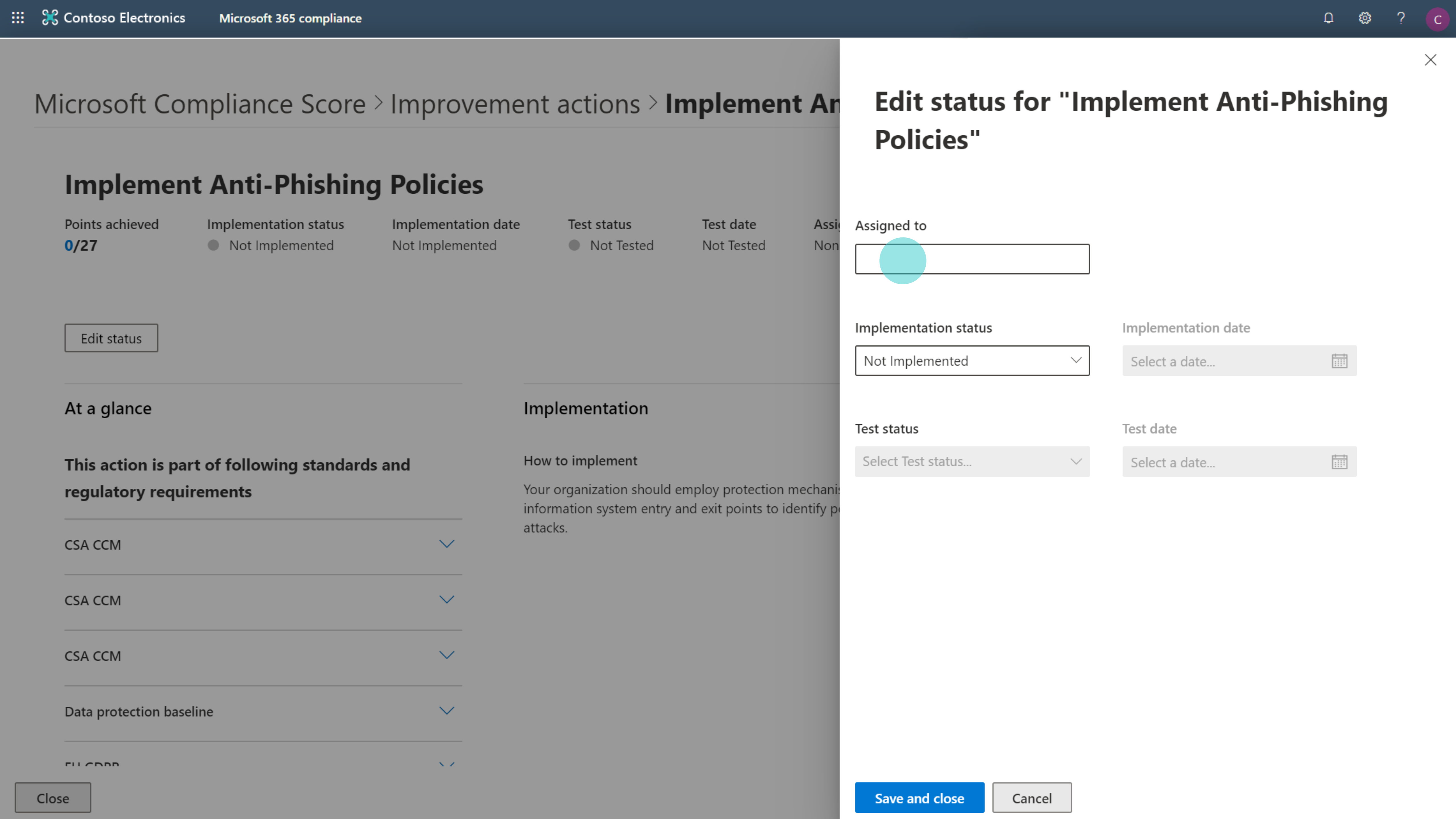
Edit implementation notes

Test notes

Edit test notes

Additional notes

Edit additional notes



Contoso Electronics

Microsoft 365 compliance

Microsoft Compliance Score > Improvement actions > Implement An

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date	Assi
0/27	● Not Implemented	Not Implemented	● Not Tested	Not Tested	Non

Edit status

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline
- EU GDPR

Implementation

How to implement

Your organization should employ protection mechanis information system entry and exit points to identify p attacks.

Close

Edit status for "Implement Anti-Phishing Policies"

Assigned to

Implementation status: Not Implemented

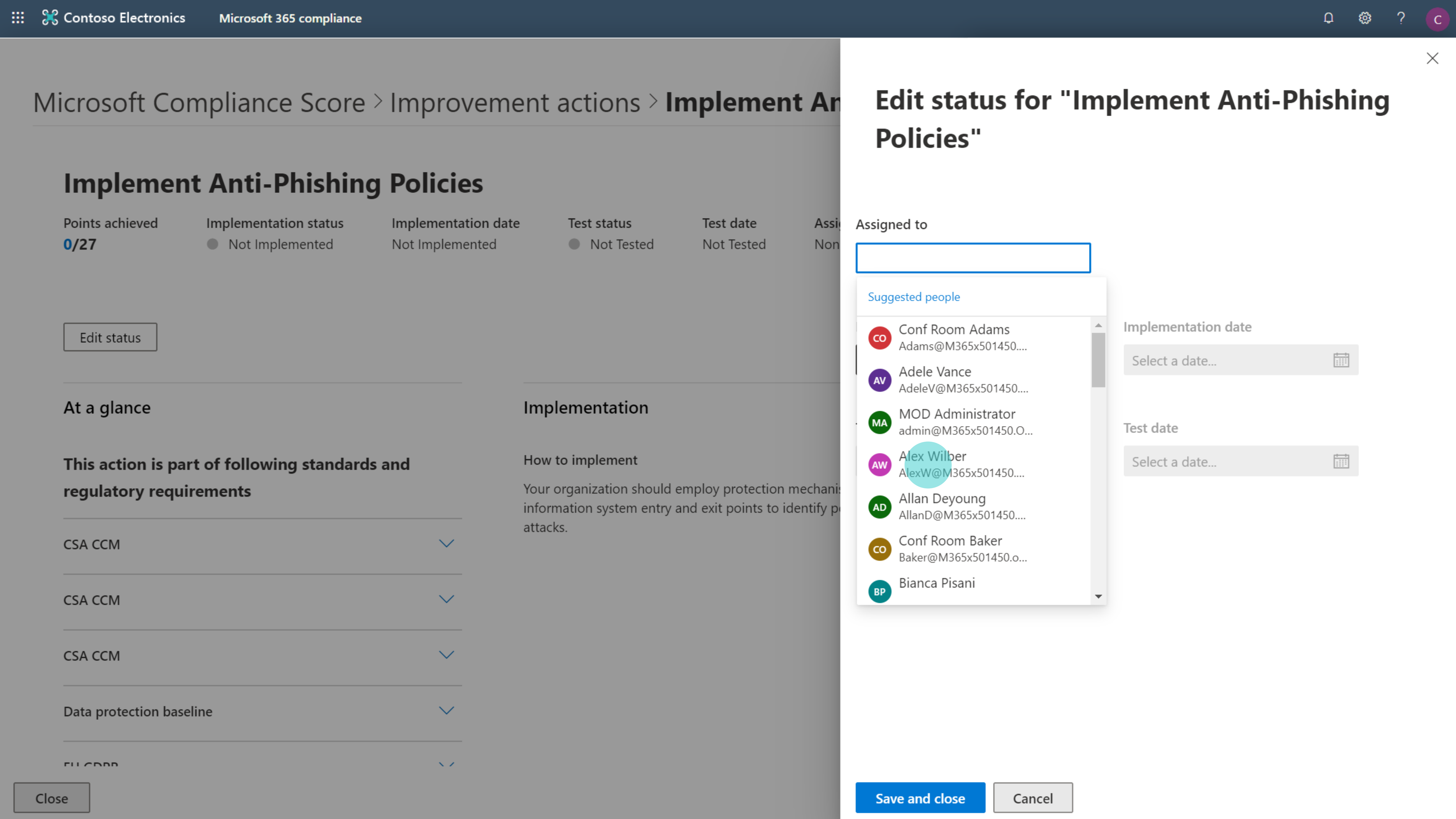
Implementation date: Select a date...

Test status: Select Test status...

Test date: Select a date...

Save and close

Cancel



Contoso Electronics Microsoft 365 compliance

Microsoft Compliance Score > Improvement actions > Implement An

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date	Assi
0/27	● Not Implemented	Not Implemented	● Not Tested	Not Tested	Non

Edit status

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline
- EU GDPR

Implementation

How to implement

Your organization should employ protection mechanis information system entry and exit points to identify p attacks.

Close

Edit status for "Implement Anti-Phishing Policies"

Assigned to

Suggested people

CO	Conf Room Adams Adams@M365x501450....
AV	Adele Vance AdeleV@M365x501450....
MA	MOD Administrator admin@M365x501450.O...
AW	Alex Wilber AlexW@M365x501450....
AD	Allan Deyoung AllanD@M365x501450....
CO	Conf Room Baker Baker@M365x501450.o...
BP	Bianca Pisani

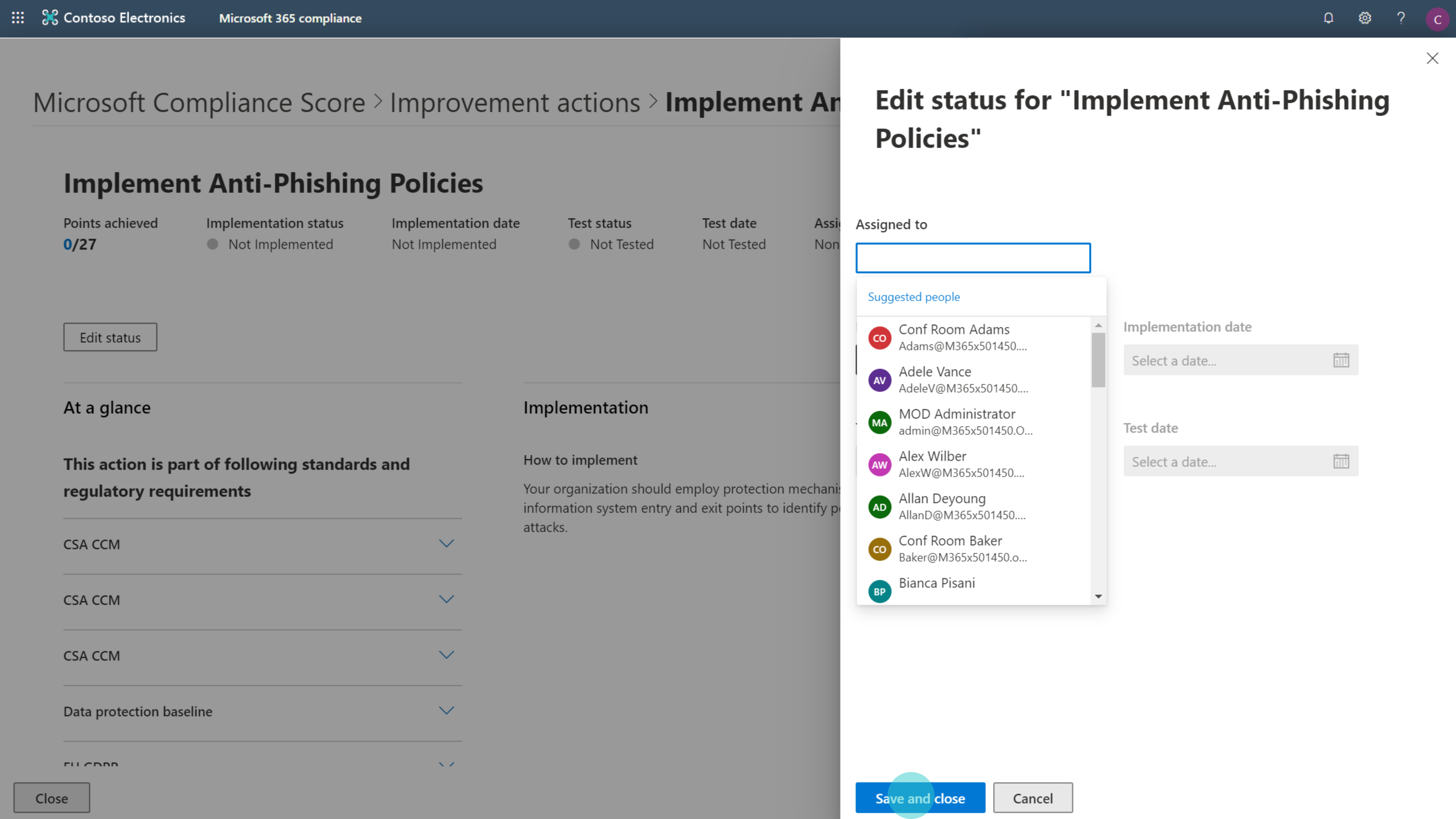
Implementation date

Select a date...

Test date

Select a date...

Save and close Cancel



Microsoft Compliance Score > Improvement actions > Implement An

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date	Assi
0/27	● Not Implemented	Not Implemented	● Not Tested	Not Tested	Non

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline
- EU GDPR

Implementation

How to implement

Your organization should employ protection mechanis information system entry and exit points to identify p attacks.

Edit status for "Implement Anti-Phishing Policies"

Assigned to

Suggested people

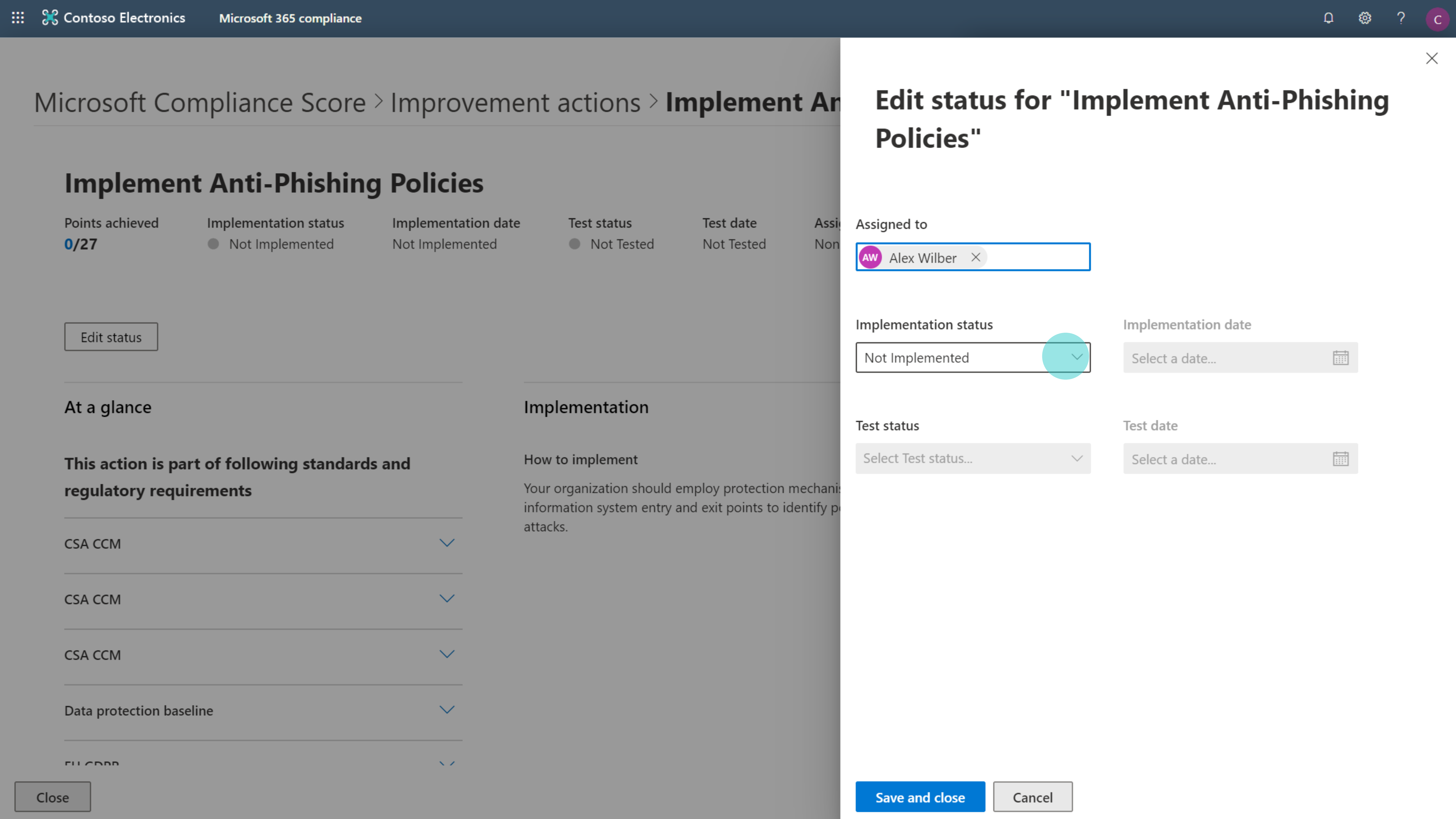
- CO Conf Room Adams Adams@M365x501450....
- AV Adele Vance AdeleV@M365x501450....
- MA MOD Administrator admin@M365x501450.O...
- AW Alex Wilber AlexW@M365x501450....
- AD Allan Deyoung AllanD@M365x501450....
- CO Conf Room Baker Baker@M365x501450.o...
- BP Bianca Pisani

Implementation date

Select a date...

Test date

Select a date...



Microsoft Compliance Score > Improvement actions > Implement An

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date	Assi
0/27	● Not Implemented	Not Implemented	● Not Tested	Not Tested	Non

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline
- EU GDPR

Implementation

How to implement

Your organization should employ protection mechanis information system entry and exit points to identify p attacks.

Edit status for "Implement Anti-Phishing Policies"

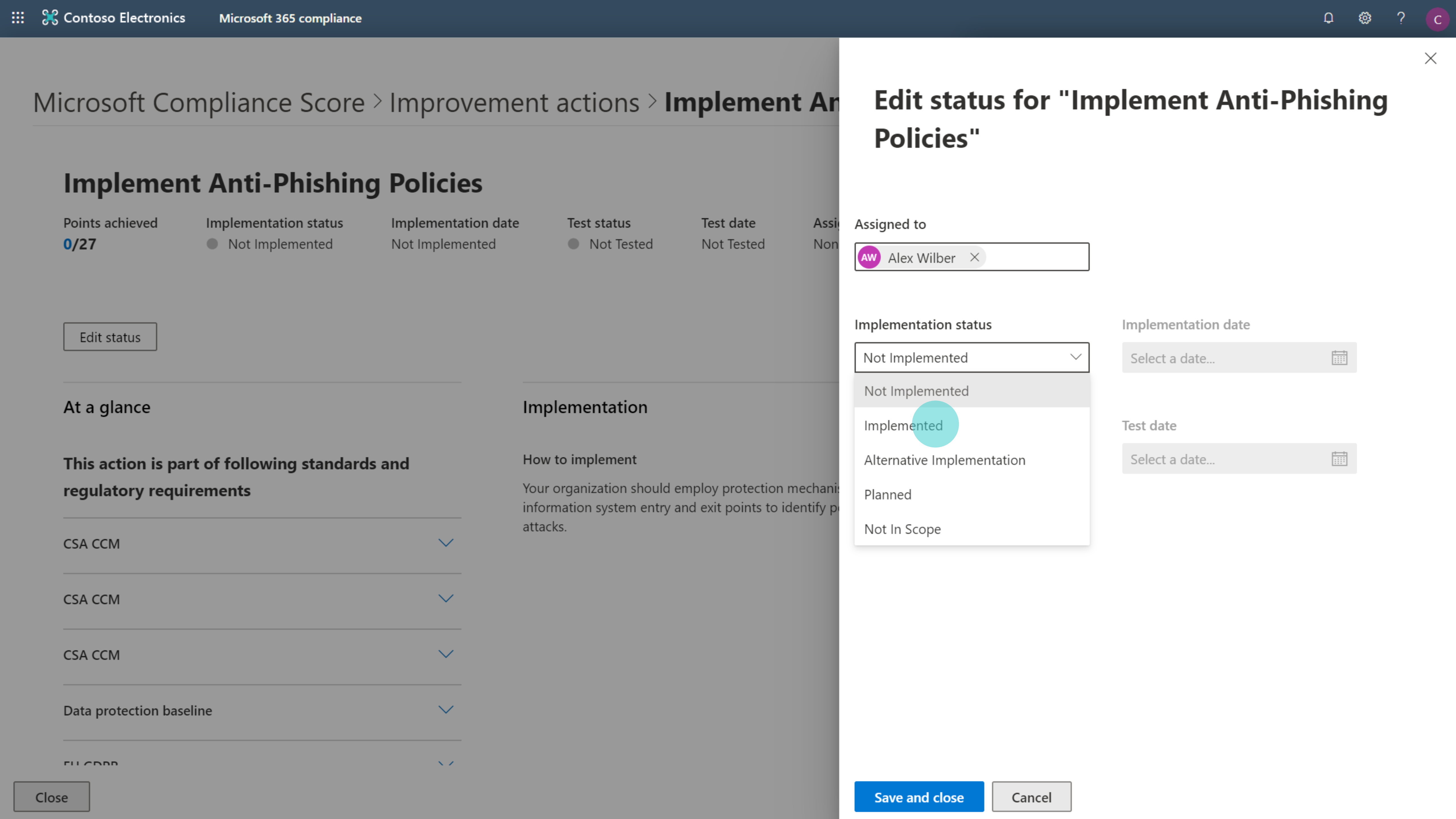
Assigned to: AW Alex Wilber ✕

Implementation status: Not Implemented

Implementation date: Select a date...

Test status: Select Test status...

Test date: Select a date...



Microsoft Compliance Score > Improvement actions > Implement An

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date	Assi
0/27	● Not Implemented	Not Implemented	● Not Tested	Not Tested	Non

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline
- EU GDPR

Implementation

How to implement

Your organization should employ protection mechanis information system entry and exit points to identify p attacks.

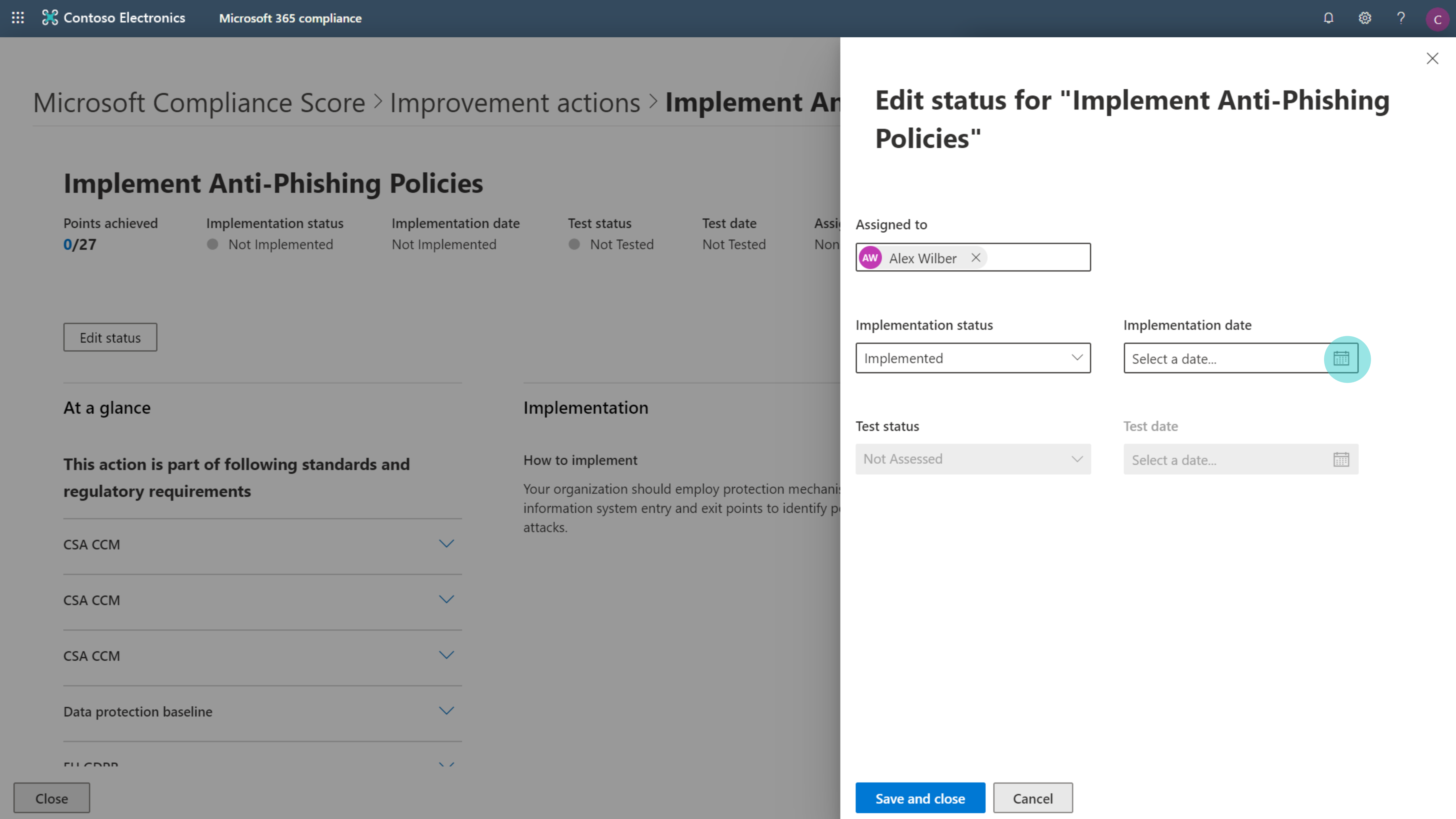
Edit status for "Implement Anti-Phishing Policies"

Assigned to: AW Alex Wilber

Implementation status: Not Implemented

Implementation date: Select a date...

Test date: Select a date...



Microsoft Compliance Score > Improvement actions > Implement An

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date	Assi
0/27	● Not Implemented	Not Implemented	● Not Tested	Not Tested	Non

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline
- EU GDPR

Implementation

How to implement

Your organization should employ protection mechanis information system entry and exit points to identify p attacks.

Edit status for "Implement Anti-Phishing Policies"

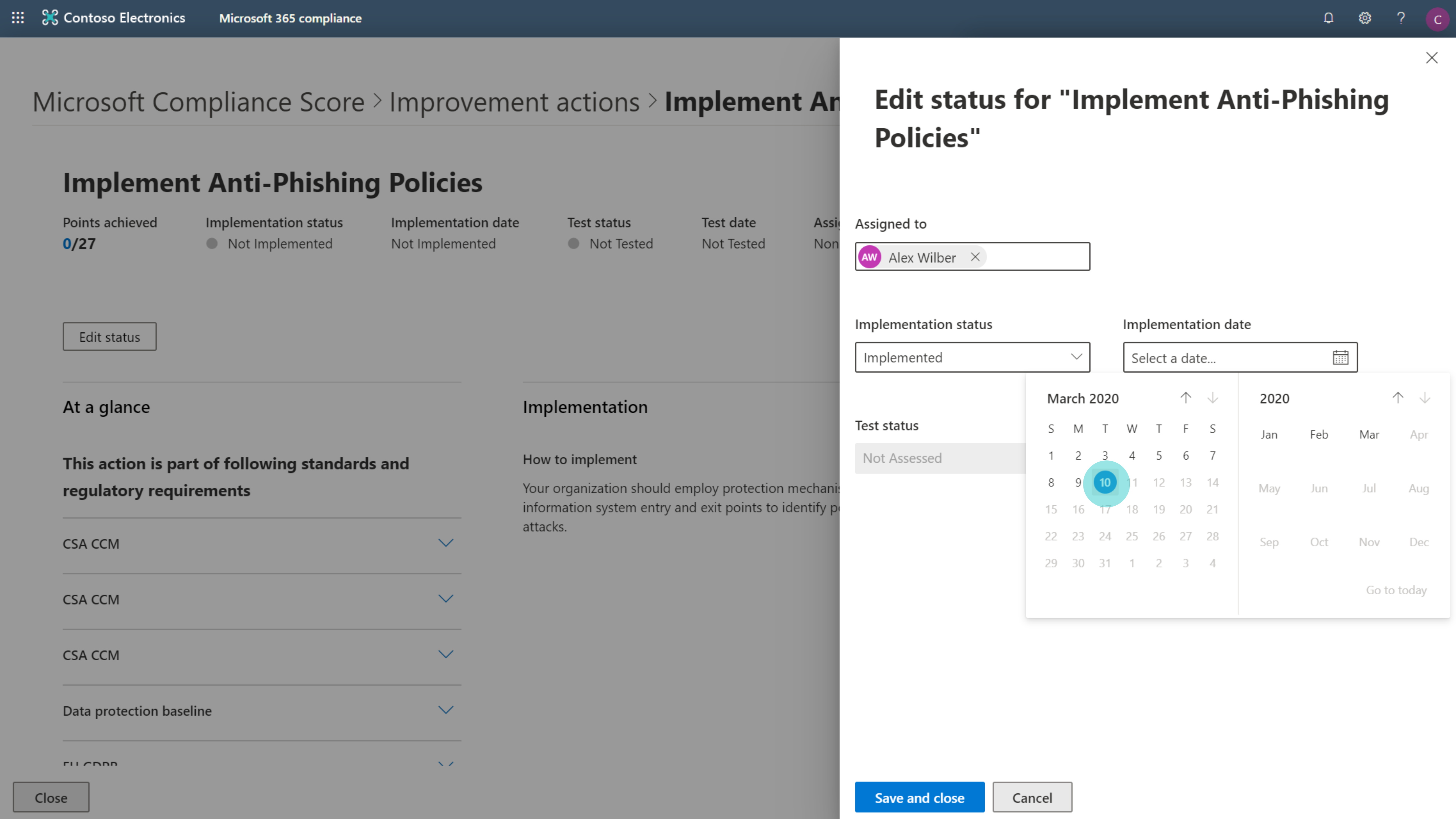
Assigned to: AW Alex Wilber ×

Implementation status: Implemented

Implementation date: Select a date...

Test status: Not Assessed

Test date: Select a date...



Microsoft Compliance Score > Improvement actions > Implement An

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date	Assi
0/27	● Not Implemented	Not Implemented	● Not Tested	Not Tested	Non

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline
- EU GDPR

Implementation

How to implement

Your organization should employ protection mechanis information system entry and exit points to identify p attacks.

Edit status for "Implement Anti-Phishing Policies"

Assigned to: AW Alex Wilber ✕

Implementation status: Implemented

Implementation date: Select a date...

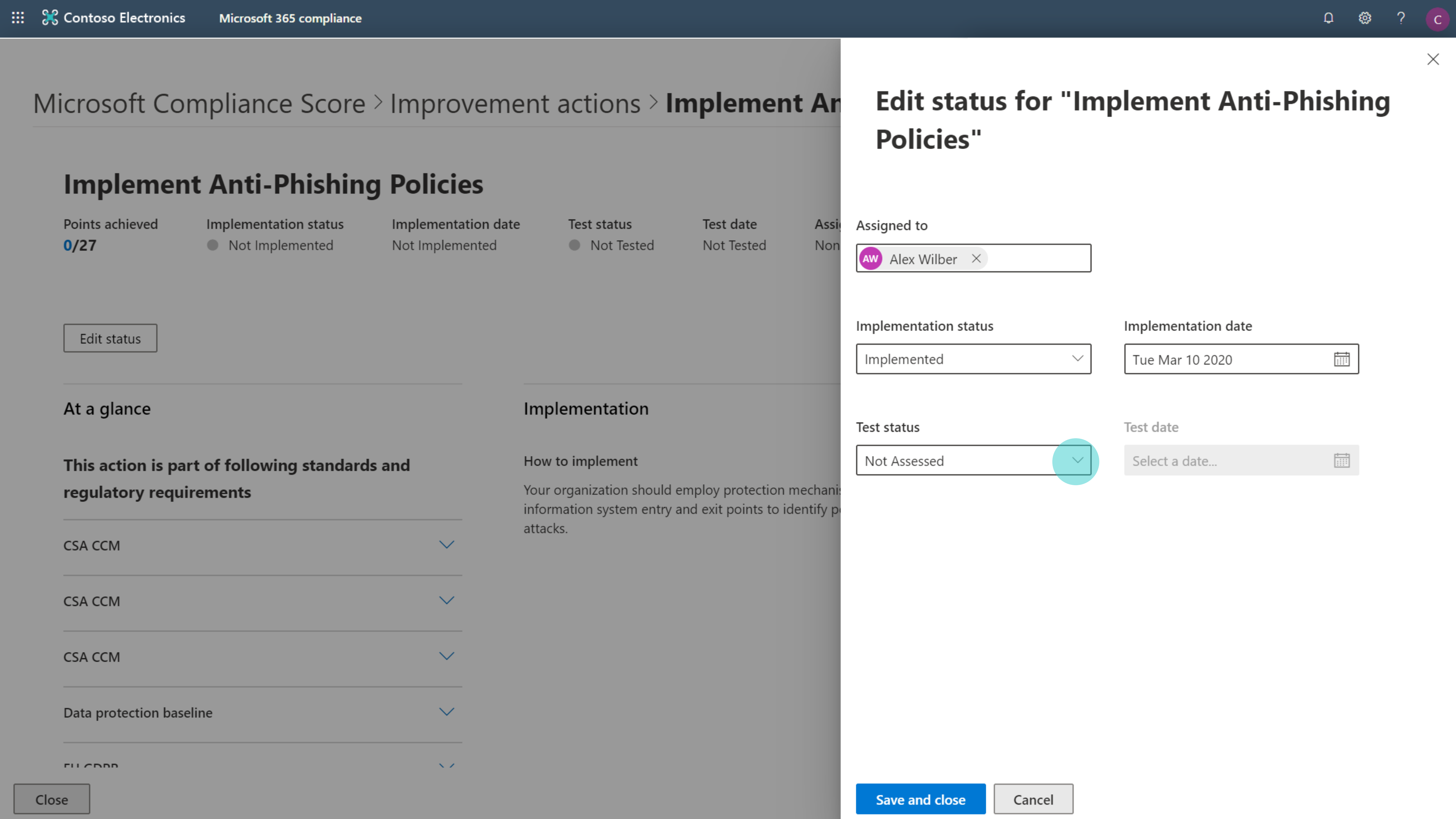
Test status: Not Assessed

March 2020

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

2020

Jan	Feb	Mar	Apr
May	Jun	Jul	Aug
Sep	Oct	Nov	Dec



Contoso Electronics Microsoft 365 compliance

Microsoft Compliance Score > Improvement actions > Implement An

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date	Assi
0/27	● Not Implemented	Not Implemented	● Not Tested	Not Tested	Non

Edit status

At a glance

This action is part of following standards and regulatory requirements

CSA CCM

CSA CCM

CSA CCM

Data protection baseline

EU GDPR

Implementation

How to implement

Your organization should employ protection mechanis information system entry and exit points to identify p attacks.

Close

Edit status for "Implement Anti-Phishing Policies"

Assigned to: AW Alex Wilber

Implementation status: Implemented

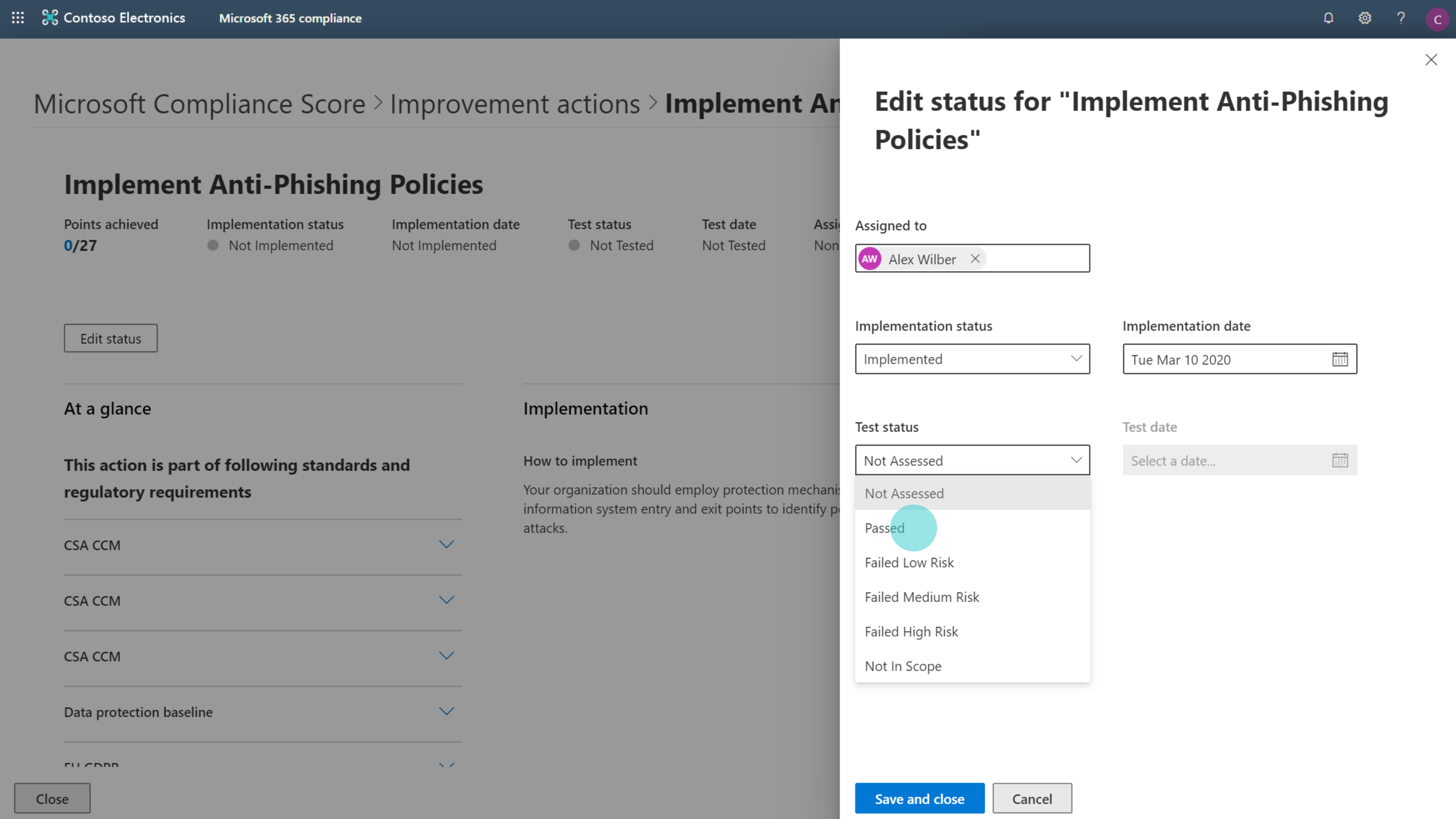
Implementation date: Tue Mar 10 2020

Test status: Not Assessed

Test date: Select a date...

Save and close

Cancel



Contoso Electronics   Microsoft 365 compliance

Microsoft Compliance Score > Improvement actions > Implement An

Implement Anti-Phishing Policies

Points achieved: 0/27

Implementation status: ● Not Implemented

Implementation date: Not Implemented

Test status: ● Not Tested

Test date: Not Tested

Assi Non

Edit status

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline
- EU GDPR

Implementation

How to implement

Your organization should employ protection mechanis information system entry and exit points to identify p attacks.

Close

Edit status for "Implement Anti-Phishing Policies"

Assigned to: AW Alex Wilber ✕

Implementation status: Implemented

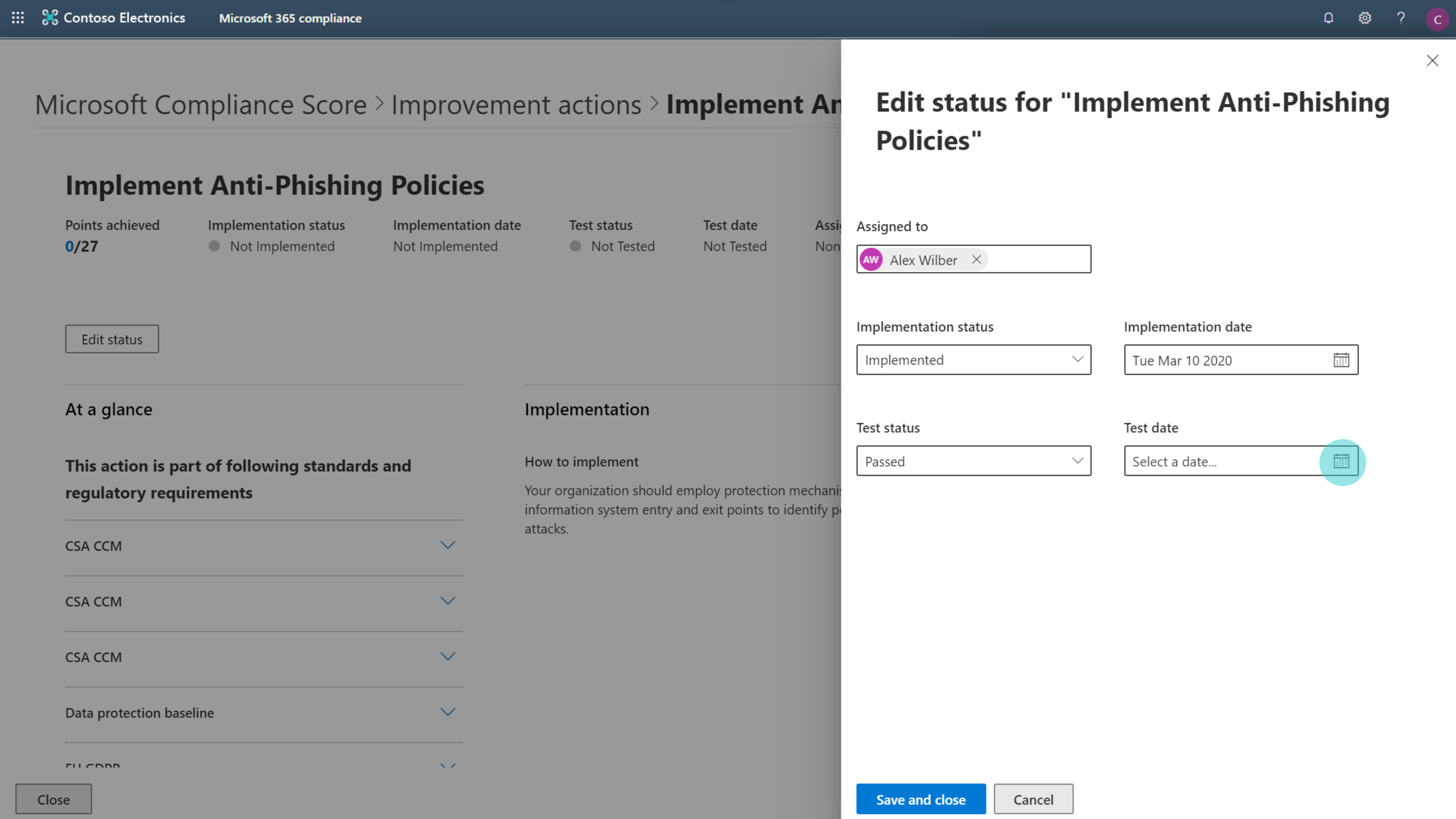
Implementation date: Tue Mar 10 2020

Test status: Not Assessed

Test date: Select a date...

- Not Assessed
- Passed
- Failed Low Risk
- Failed Medium Risk
- Failed High Risk
- Not In Scope

Save and close   Cancel



Microsoft Compliance Score > Improvement actions > Implement An

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date	Assi
0/27	● Not Implemented	Not Implemented	● Not Tested	Not Tested	Non

Edit status

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline
- EU GDPR

Implementation

How to implement

Your organization should employ protection mechanis information system entry and exit points to identify p attacks.

Close

Edit status for "Implement Anti-Phishing Policies"

Assigned to: AW Alex Wilber ✕

Implementation status: Implemented

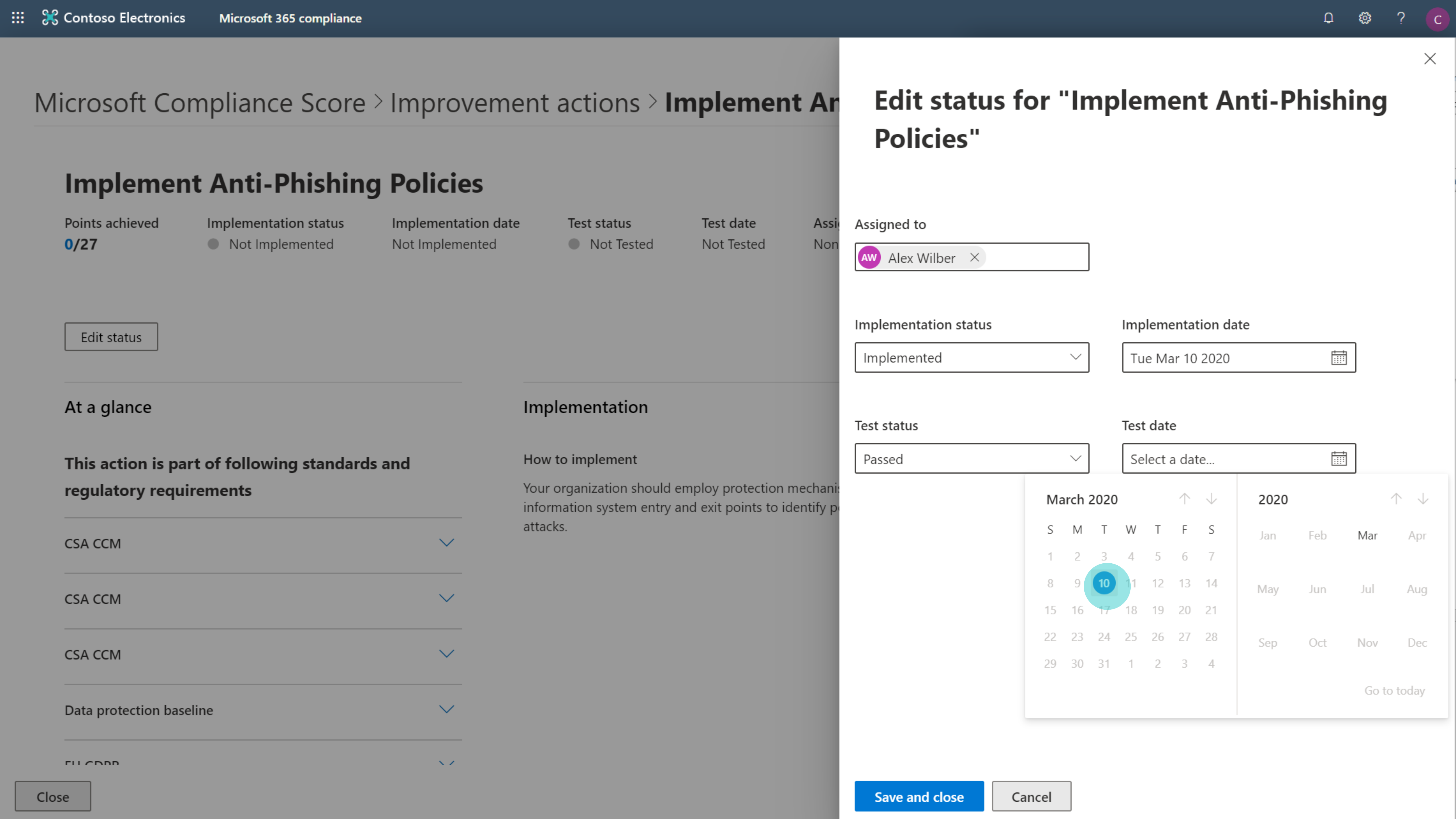
Implementation date: Tue Mar 10 2020

Test status: Passed

Test date: Select a date...

Save and close

Cancel



Microsoft Compliance Score > Improvement actions > Implement An

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date	Assi
0/27	● Not Implemented	Not Implemented	● Not Tested	Not Tested	Non

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline
- EU GDPR

Implementation

How to implement

Your organization should employ protection mechanis information system entry and exit points to identify p attacks.

Edit status for "Implement Anti-Phishing Policies"

Assigned to: AW Alex Wilber ✕

Implementation status: Implemented

Implementation date: Tue Mar 10 2020

Test status: Passed

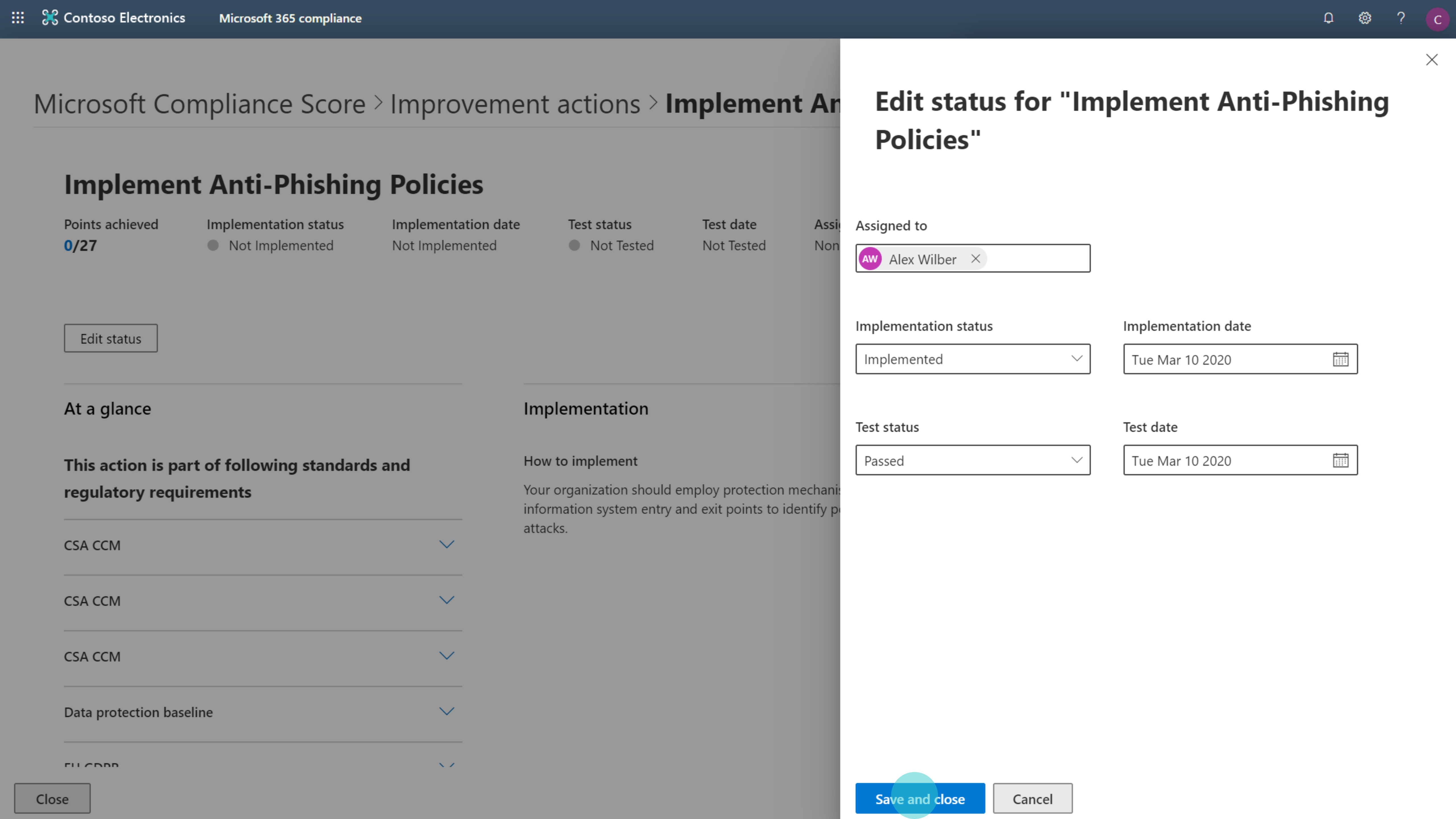
Test date: Select a date...

March 2020

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

2020

Jan	Feb	Mar	Apr
May	Jun	Jul	Aug
Sep	Oct	Nov	Dec



Microsoft Compliance Score > Improvement actions > Implement An

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date	Assi
0/27	● Not Implemented	Not Implemented	● Not Tested	Not Tested	Non

Edit status

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline
- EU GDPR

Implementation

How to implement

Your organization should employ protection mechanis information system entry and exit points to identify p attacks.

Edit status for "Implement Anti-Phishing Policies"

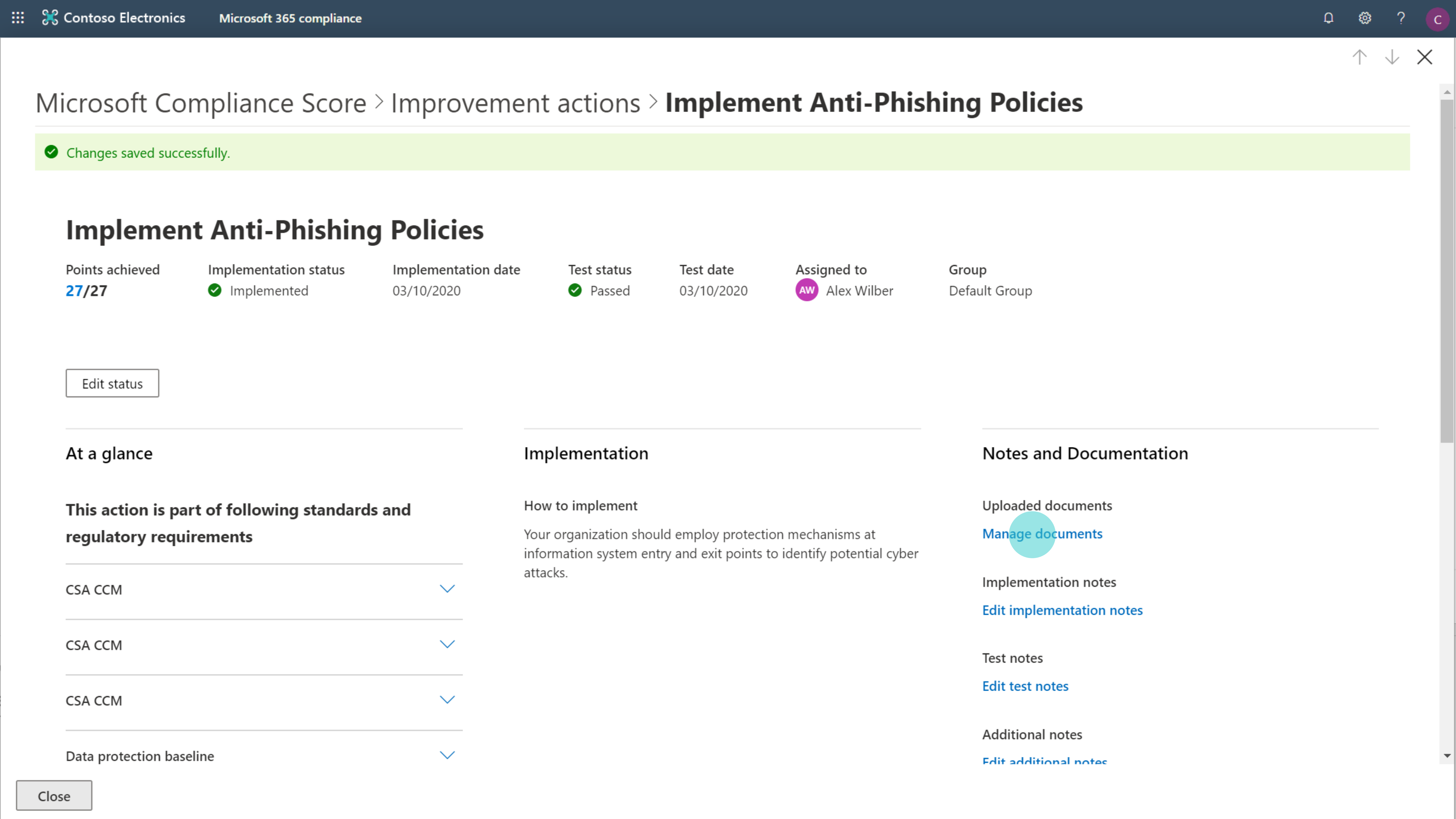
Assigned to: AW Alex Wilber ✕

Implementation status: Implemented

Implementation date: Tue Mar 10 2020

Test status: Passed

Test date: Tue Mar 10 2020



Microsoft Compliance Score > Improvement actions > **Implement Anti-Phishing Policies**

✓ Changes saved successfully.

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date	Assigned to	Group
27/27	✓ Implemented	03/10/2020	✓ Passed	03/10/2020	AW Alex Wilber	Default Group

Edit status

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline

Implementation

How to implement

Your organization should employ protection mechanisms at information system entry and exit points to identify potential cyber attacks.

Notes and Documentation

Uploaded documents

Manage documents

Implementation notes

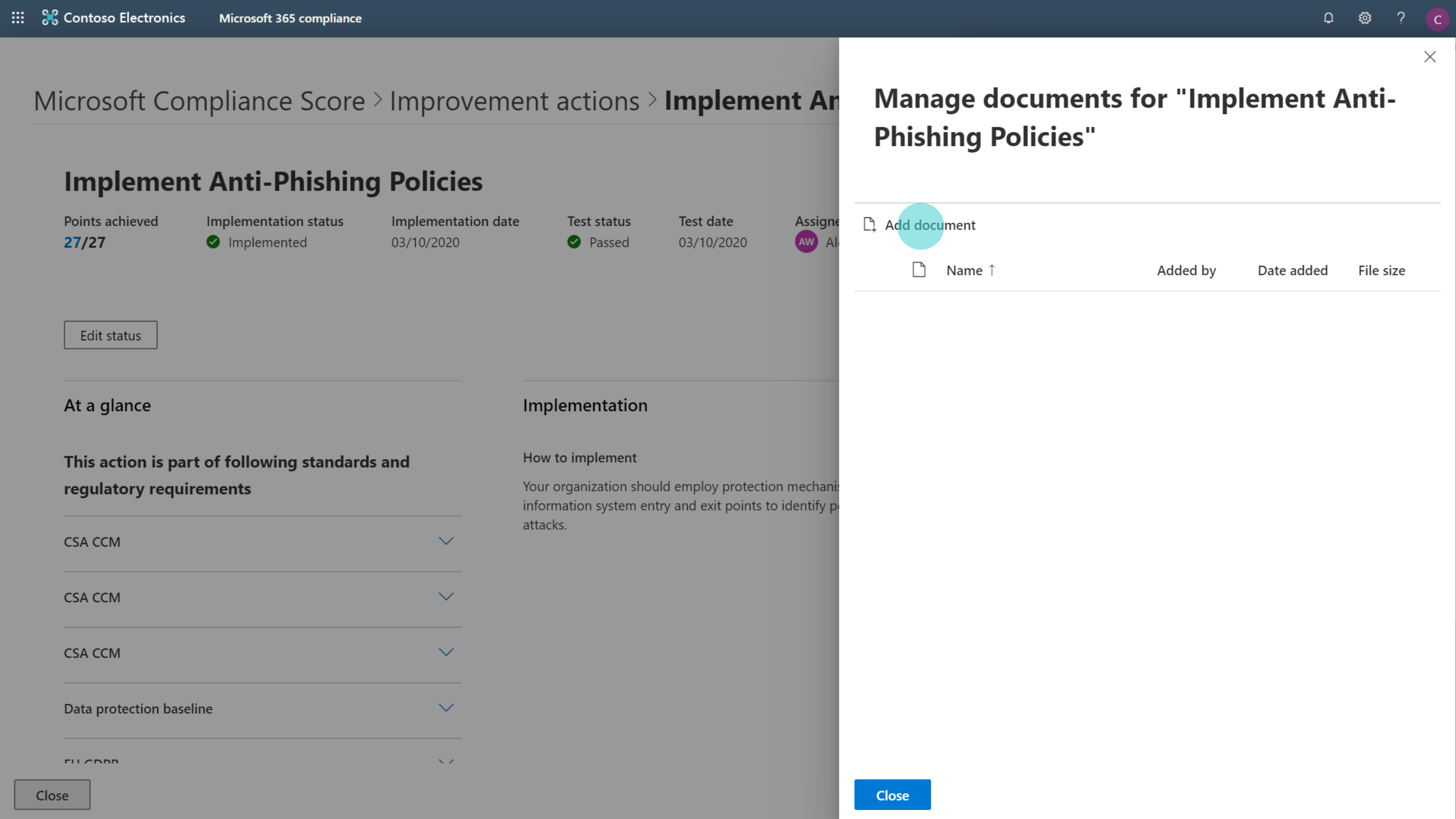
Edit implementation notes

Test notes

Edit test notes

Additional notes

Edit additional notes



Microsoft Compliance Score > Improvement actions > Implement An

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date	Assigne
27/27	✓ Implemented	03/10/2020	✓ Passed	03/10/2020	AW Al

Edit status

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline
- EU GDPR

Implementation

How to implement

Your organization should employ protection mechanis information system entry and exit points to identify p attacks.

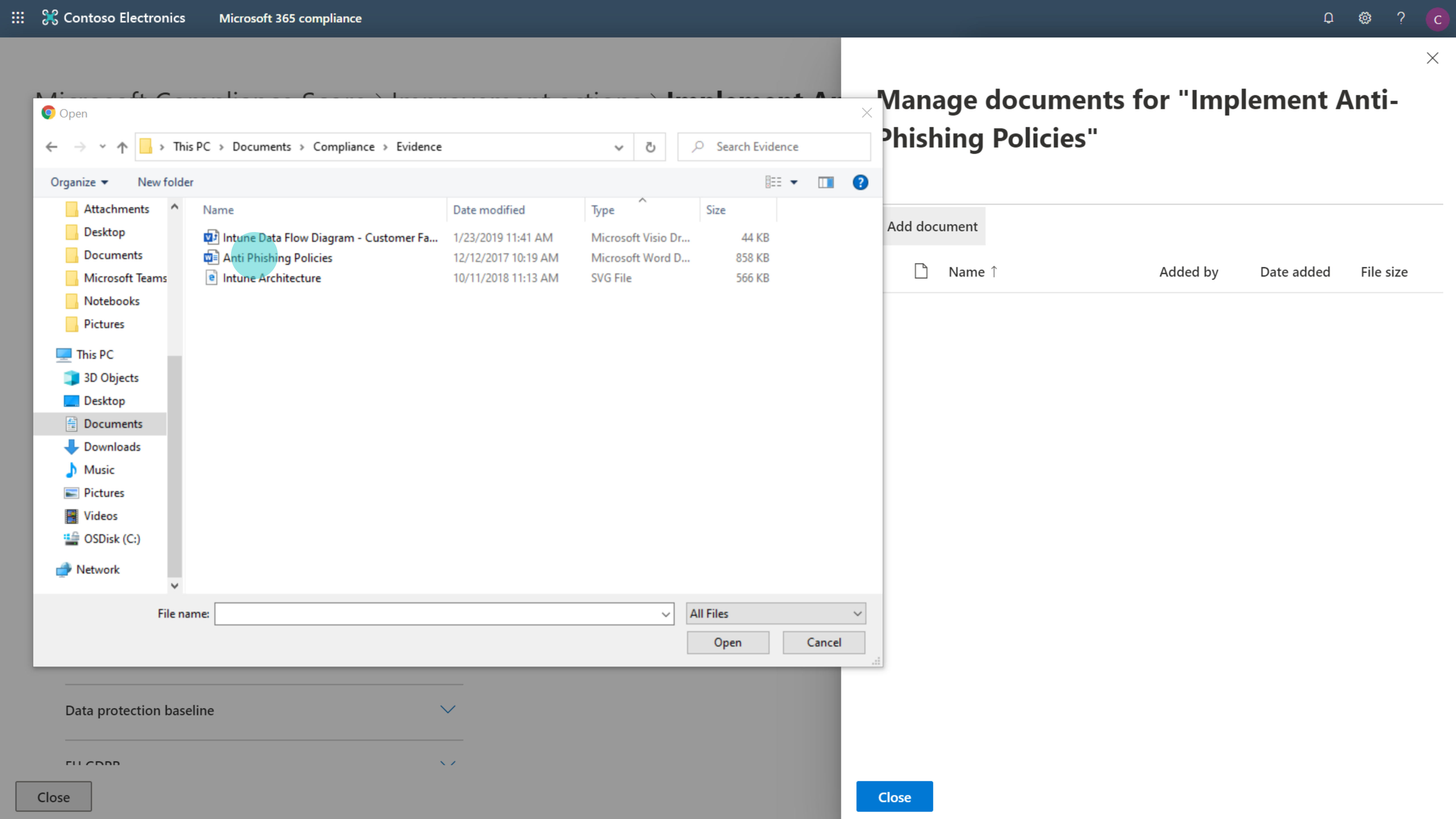
Close

Manage documents for "Implement Anti-Phishing Policies"

Add document

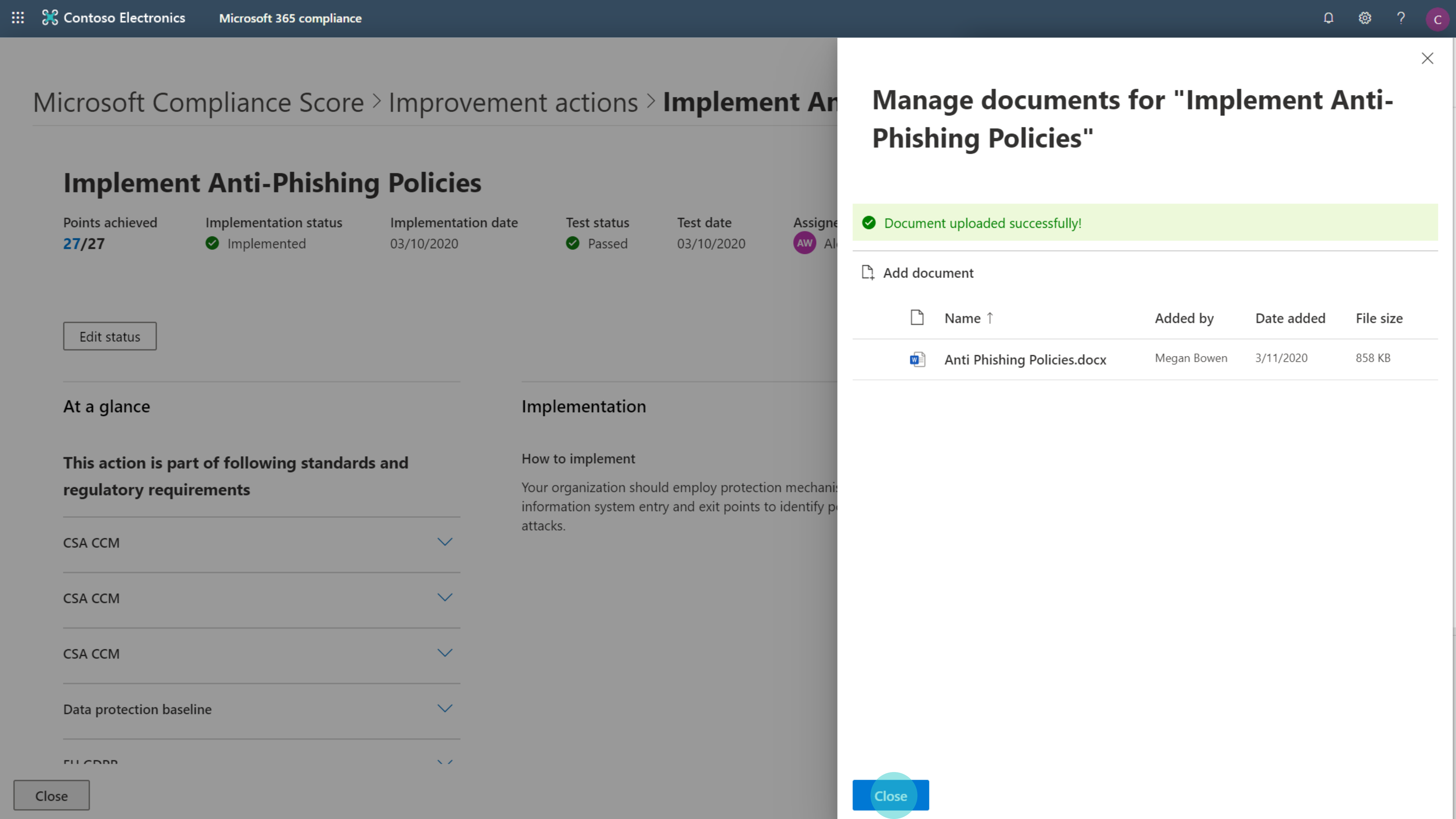
Name ↑	Added by	Date added	File size

Close



Manage documents for "Implement Anti-Phishing Policies"

Name	Date modified	Type	Size
Intune Data Flow Diagram - Customer Fa...	1/23/2019 11:41 AM	Microsoft Visio Dr...	44 KB
Anti Phishing Policies	12/12/2017 10:19 AM	Microsoft Word D...	858 KB
Intune Architecture	10/11/2018 11:13 AM	SVG File	566 KB



Microsoft Compliance Score > Improvement actions > Implement An

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date	Assigne
27/27	✓ Implemented	03/10/2020	✓ Passed	03/10/2020	AW Al

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline
- EU GDPR

Implementation

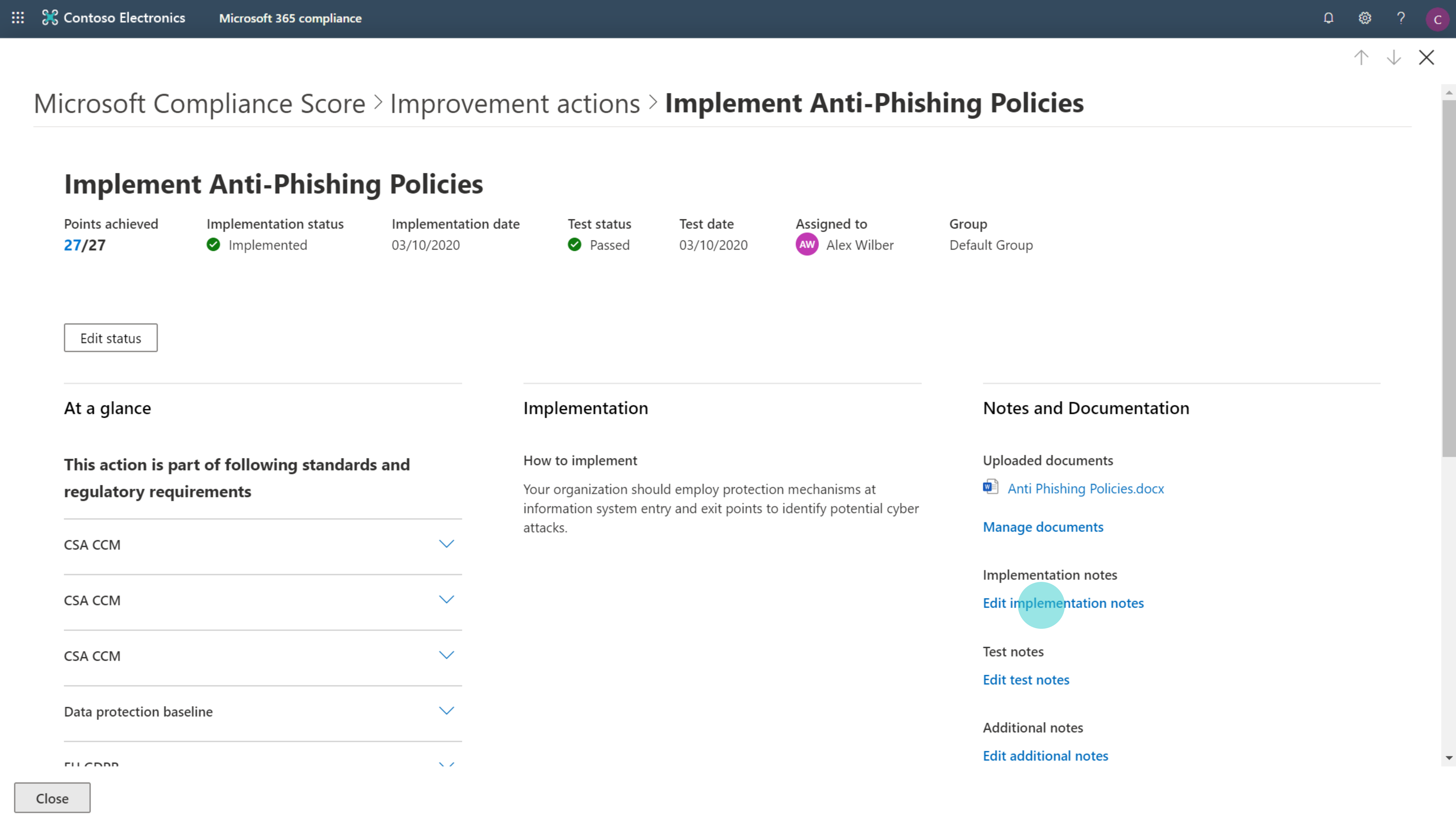
How to implement

Your organization should employ protection mechani information system entry and exit points to identify p attacks.

Manage documents for "Implement Anti-Phishing Policies"

✓ Document uploaded successfully!

Name ↑	Added by	Date added	File size
Anti Phishing Policies.docx	Megan Bowen	3/11/2020	858 KB



Microsoft Compliance Score > Improvement actions > **Implement Anti-Phishing Policies**

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date	Assigned to	Group
27/27	✓ Implemented	03/10/2020	✓ Passed	03/10/2020	AW Alex Wilber	Default Group

At a glance

This action is part of following standard and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline
- EU GDPR

Implementation

How to implement

Your organization should employ protection mechanisms at information system entry and exit points to identify potential cyber attacks.

Notes and Documentation

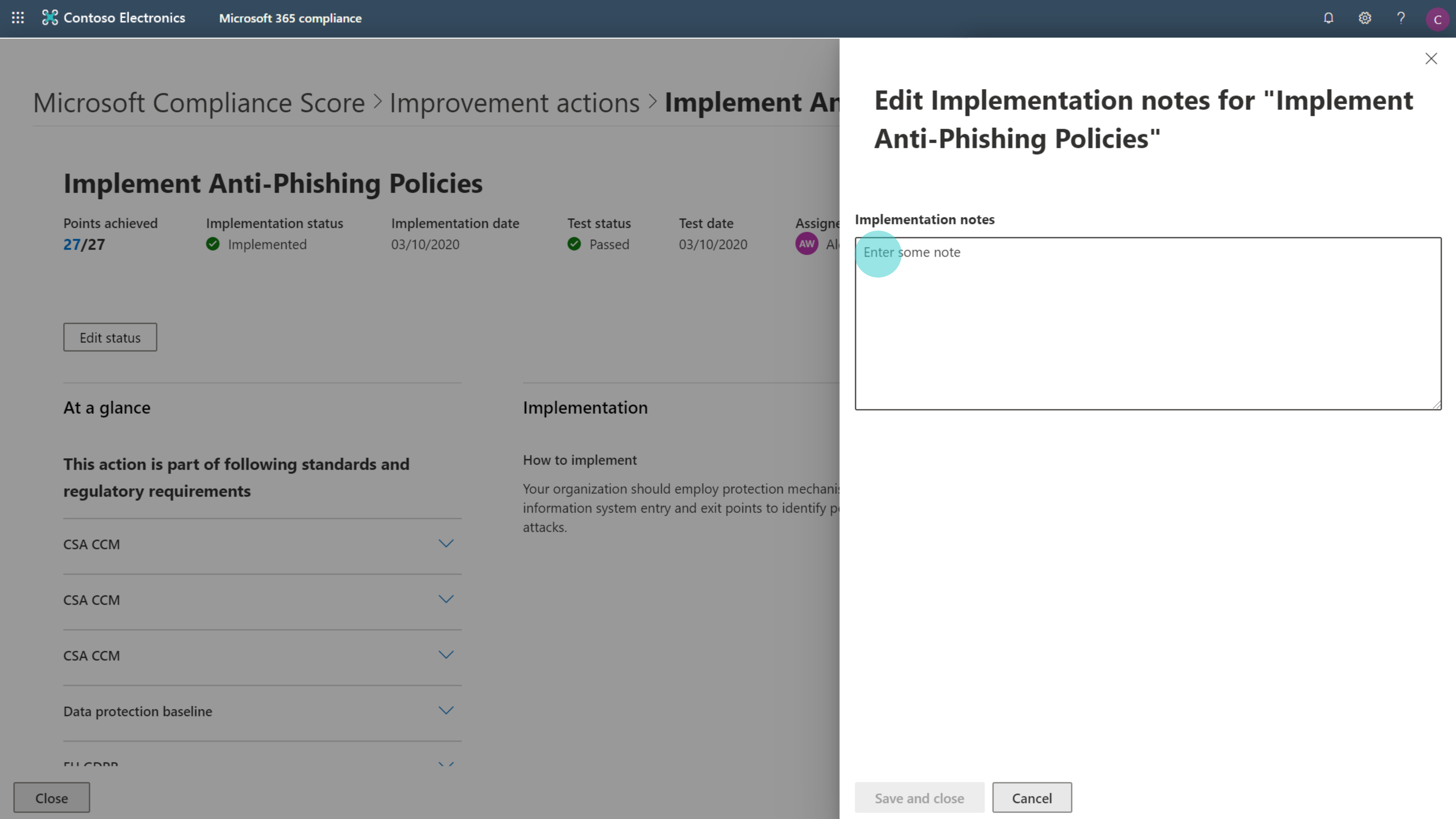
Uploaded documents

Anti Phishing Policies.docx

Implementation notes

Test notes

Additional notes



Microsoft Compliance Score > Improvement actions > Implement An

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date	Assigne
27/27	✓ Implemented	03/10/2020	✓ Passed	03/10/2020	AW Al

Edit status

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline
- EU GDPR

Implementation

How to implement

Your organization should employ protection mechanis information system entry and exit points to identify p attacks.

Close

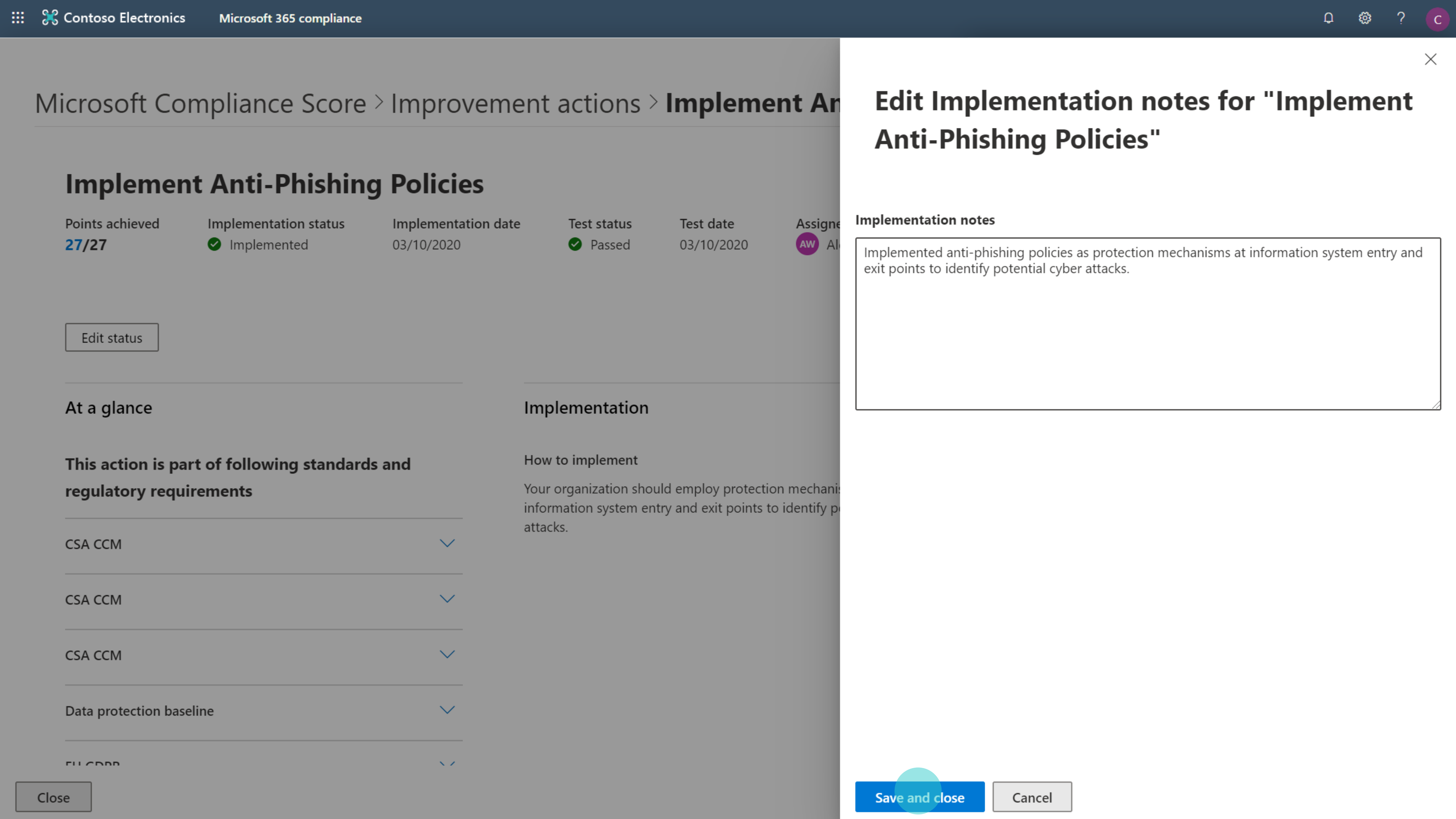
Edit Implementation notes for "Implement Anti-Phishing Policies"

Implementation notes

Enter some note

Save and close

Cancel



Microsoft Compliance Score > Improvement actions > Implement An

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date	Assigne
27/27	✓ Implemented	03/10/2020	✓ Passed	03/10/2020	AW Al

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline
- EU GDPR

Implementation

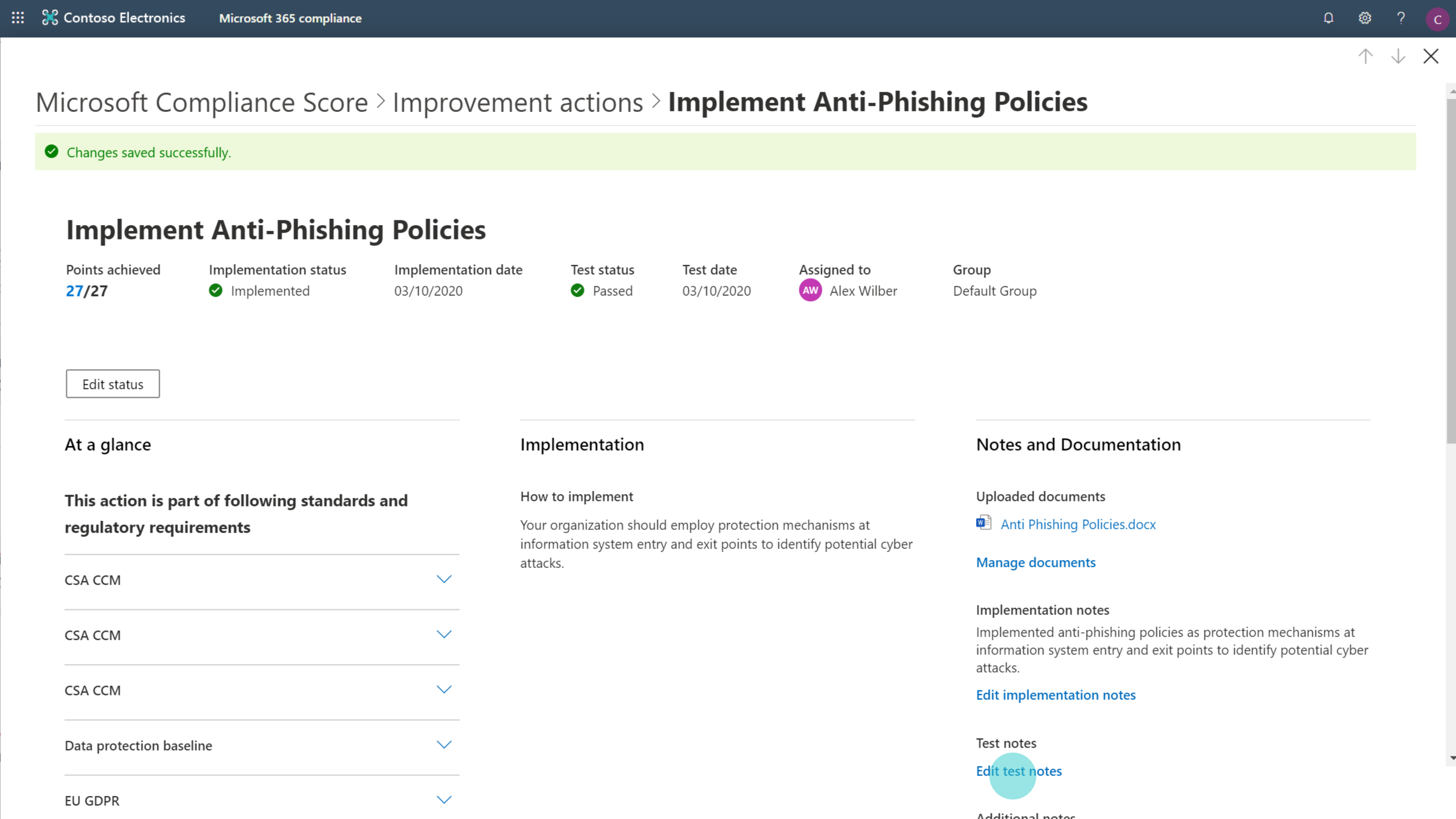
How to implement

Your organization should employ protection mechanis information system entry and exit points to identify p attacks.

Edit Implementation notes for "Implement Anti-Phishing Policies"

Implementation notes

Implemented anti-phishing policies as protection mechanisms at information system entry and exit points to identify potential cyber attacks.



Microsoft Compliance Score > Improvement actions > **Implement Anti-Phishing Policies**

✓ Changes saved successfully.

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date	Assigned to	Group
27/27	✓ Implemented	03/10/2020	✓ Passed	03/10/2020	AW Alex Wilber	Default Group

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline
- EU GDPR

Implementation

How to implement

Your organization should employ protection mechanisms at information system entry and exit points to identify potential cyber attacks.

Notes and Documentation

Uploaded documents

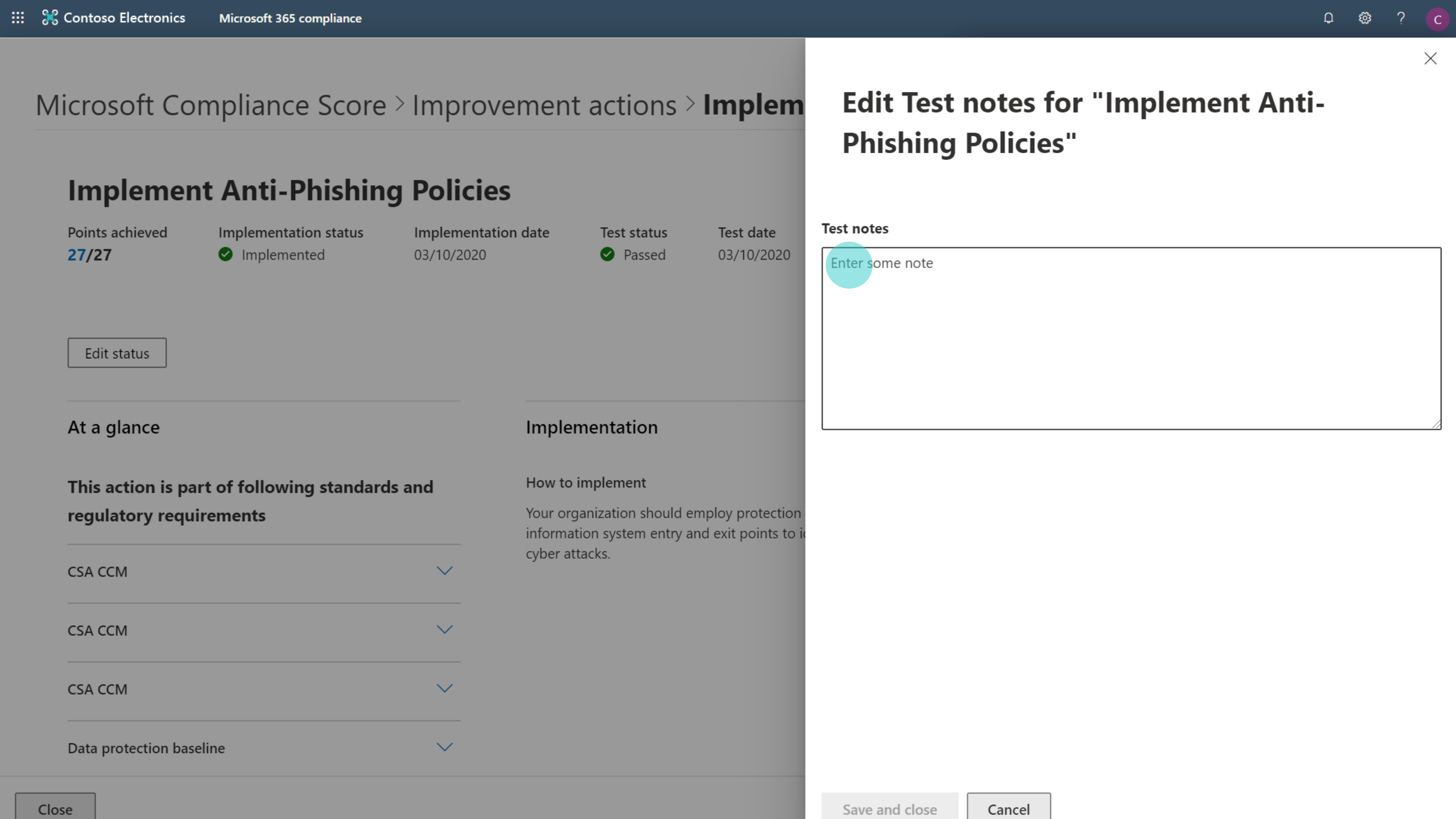
Anti Phishing Policies.docx

Implementation notes

Implemented anti-phishing policies as protection mechanisms at information system entry and exit points to identify potential cyber attacks.

Test notes

Additional notes



Microsoft Compliance Score > Improvement actions > Implem

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date
27/27	✓ Implemented	03/10/2020	✓ Passed	03/10/2020

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline

Implementation

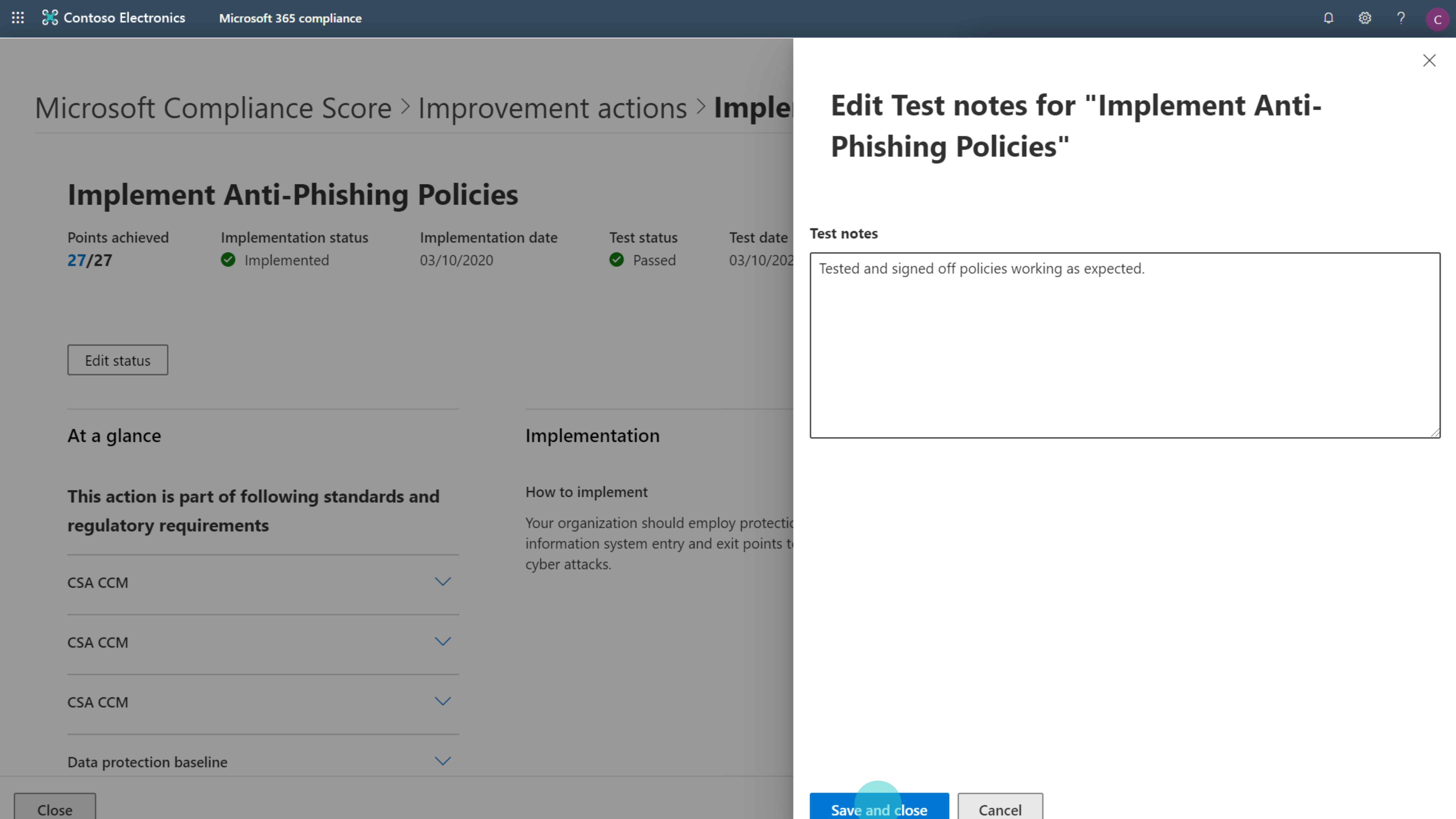
How to implement

Your organization should employ protection information system entry and exit points to i cyber attacks.

Edit Test notes for "Implement Anti-Phishing Policies"

Test notes

Enter some note



Microsoft Compliance Score > Improvement actions > Imple

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date
27/27	✓ Implemented	03/10/2020	✓ Passed	03/10/202

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline

Implementation

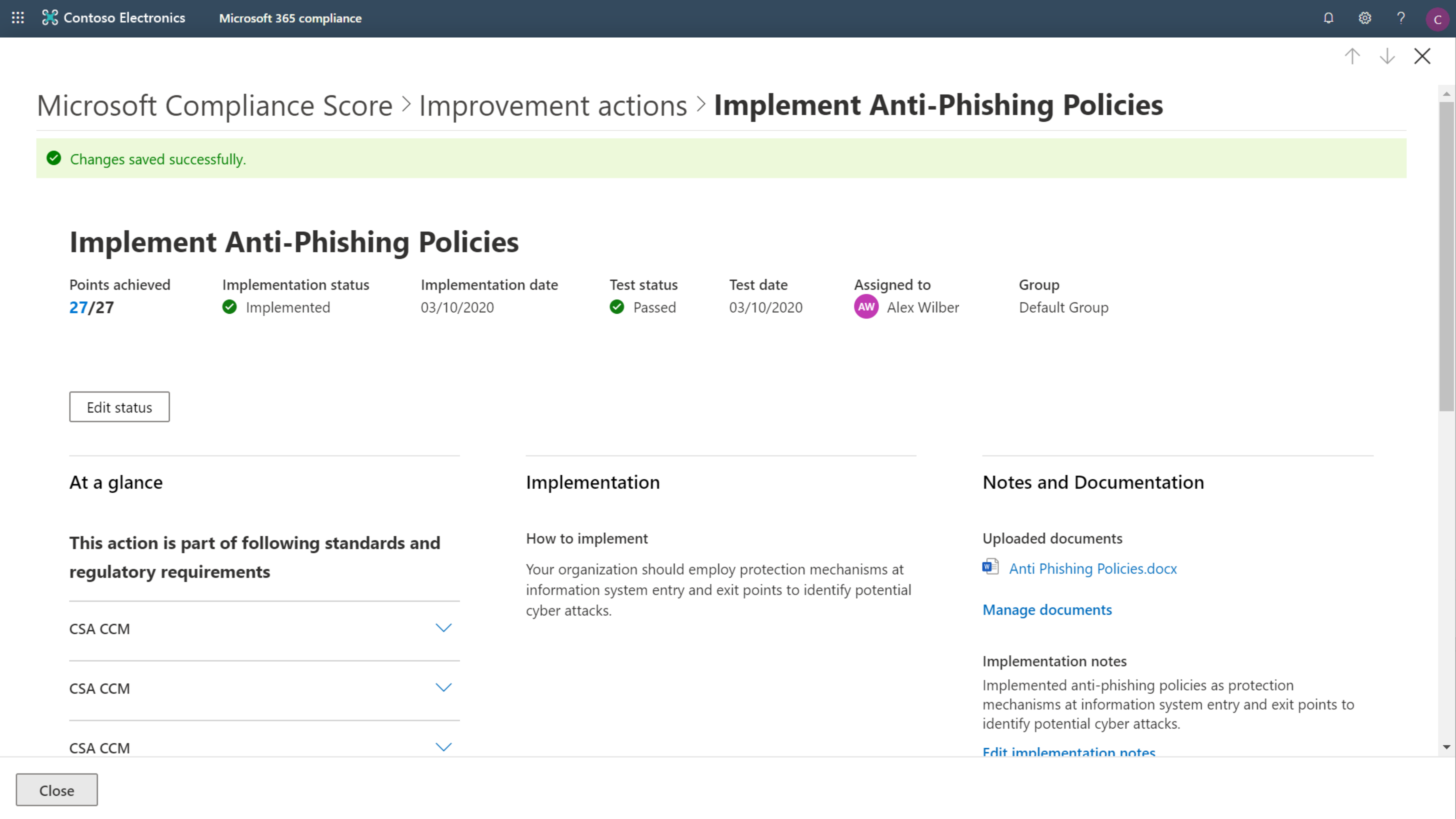
How to implement

Your organization should employ protecti
information system entry and exit points t
cyber attacks.

Edit Test notes for "Implement Anti-Phishing Policies"

Test notes

Tested and signed off policies working as expected.



Microsoft Compliance Score > Improvement actions > **Implement Anti-Phishing Policies**

✓ Changes saved successfully.

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date	Assigned to	Group
27/27	✓ Implemented	03/10/2020	✓ Passed	03/10/2020	AW Alex Wilber	Default Group

At a glance

This action is part of following standards and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM

Implementation

How to implement

Your organization should employ protection mechanisms at information system entry and exit points to identify potential cyber attacks.

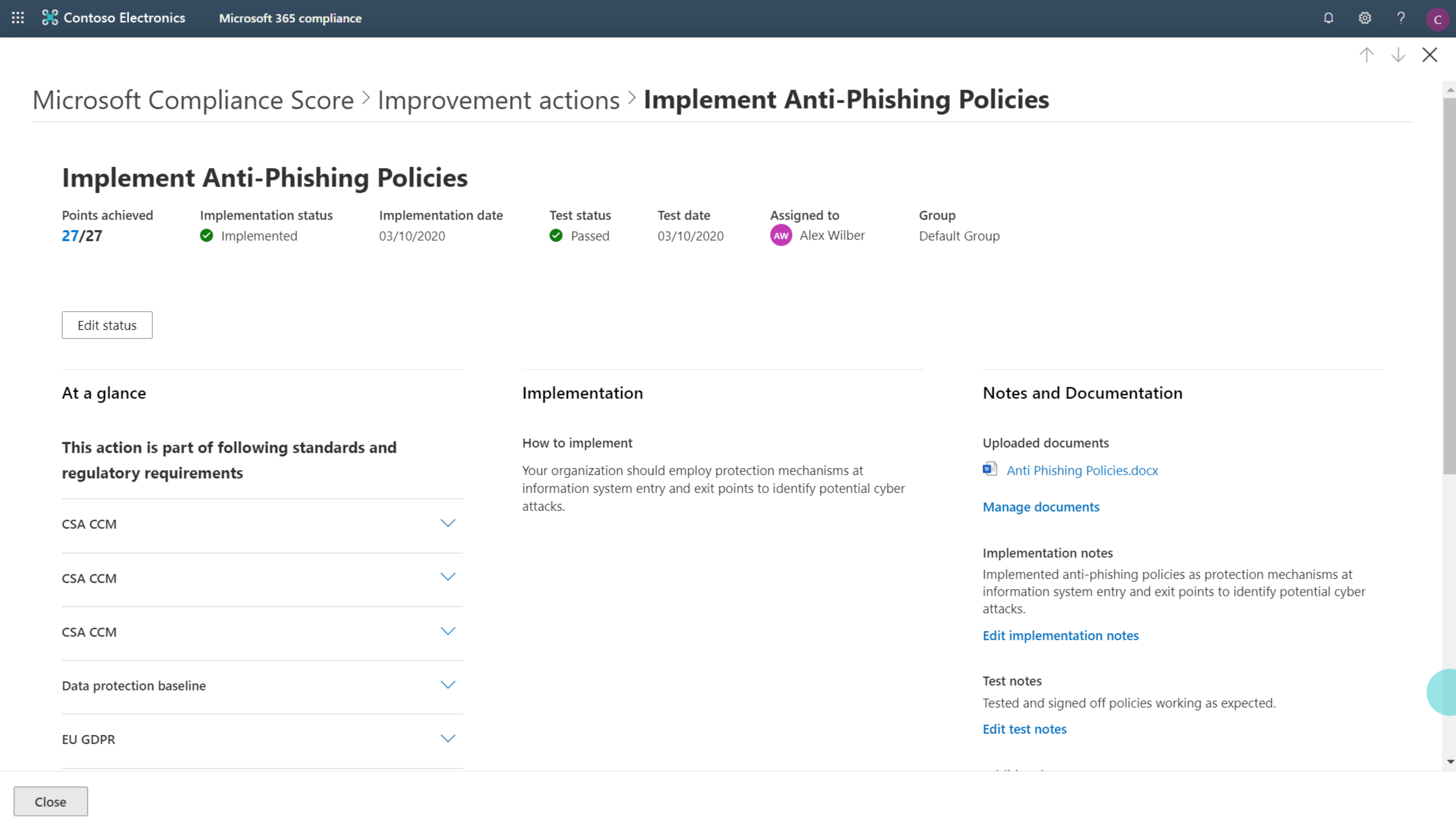
Notes and Documentation

Uploaded documents

Anti Phishing Policies.docx

Implementation notes

Implemented anti-phishing policies as protection mechanisms at information system entry and exit points to identify potential cyber attacks.



Microsoft Compliance Score > Improvement actions > **Implement Anti-Phishing Policies**

Implement Anti-Phishing Policies

Points achieved	Implementation status	Implementation date	Test status	Test date	Assigned to	Group
27/27	✓ Implemented	03/10/2020	✓ Passed	03/10/2020	AW Alex Wilber	Default Group

At a glance

This action is part of following standard and regulatory requirements

- CSA CCM
- CSA CCM
- CSA CCM
- Data protection baseline
- EU GDPR

Implementation

How to implement

Your organization should employ protection mechanisms at information system entry and exit points to identify potential cyber attacks.

Notes and Documentation

Uploaded documents

Anti Phishing Policies.docx

Manage documents

Implementation notes

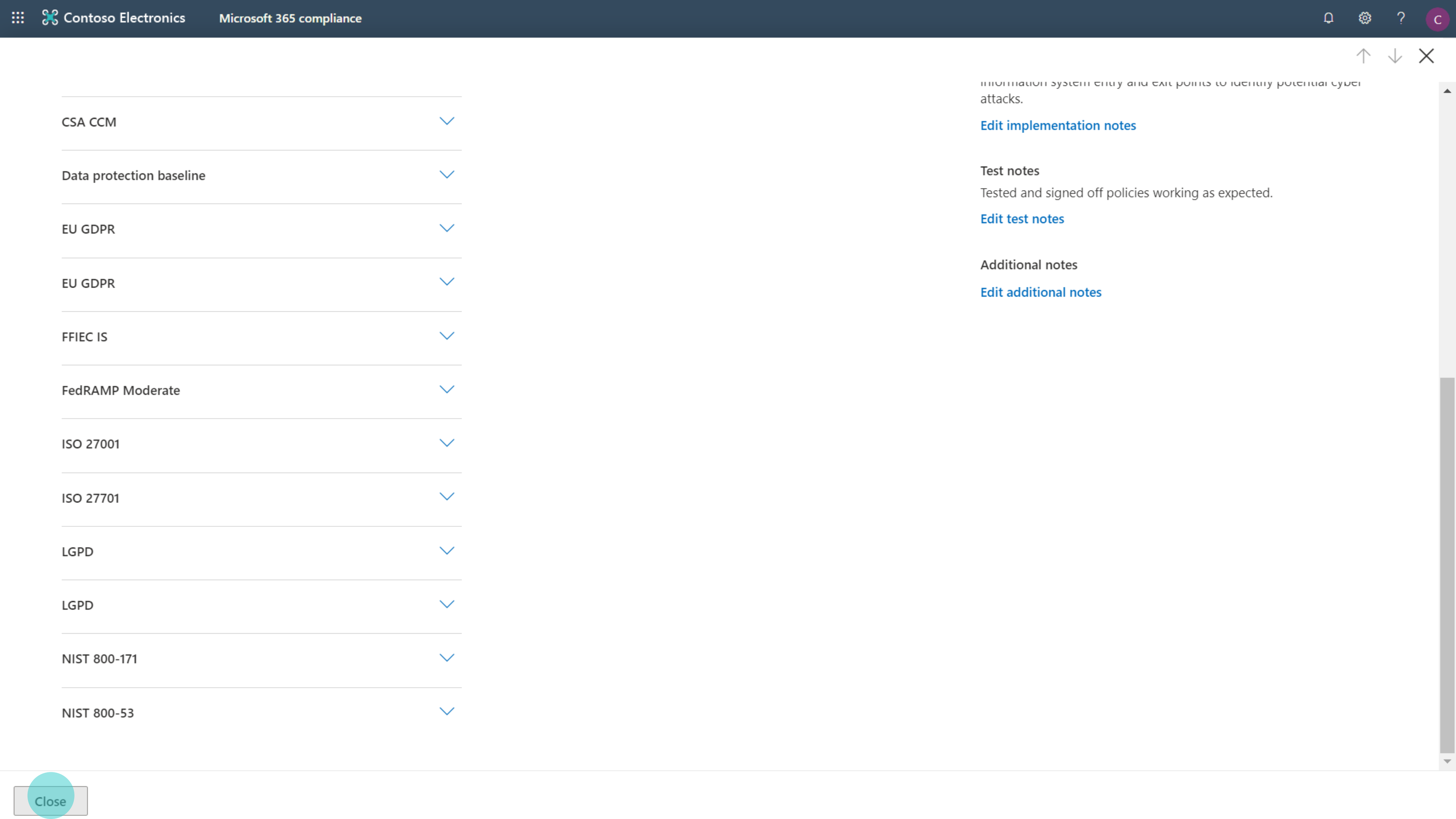
Implemented anti-phishing policies as protection mechanisms at information system entry and exit points to identify potential cyber attacks.

Edit implementation notes

Test notes

Tested and signed off policies working as expected.

Edit test notes



CSA CCM

Data protection baseline

EU GDPR

EU GDPR

FFIEC IS

FedRAMP Moderate

ISO 27001

ISO 27701

LGPD

LGPD

NIST 800-171

NIST 800-53

information system entry and exit points to identify potential cyber attacks.

Edit implementation notes

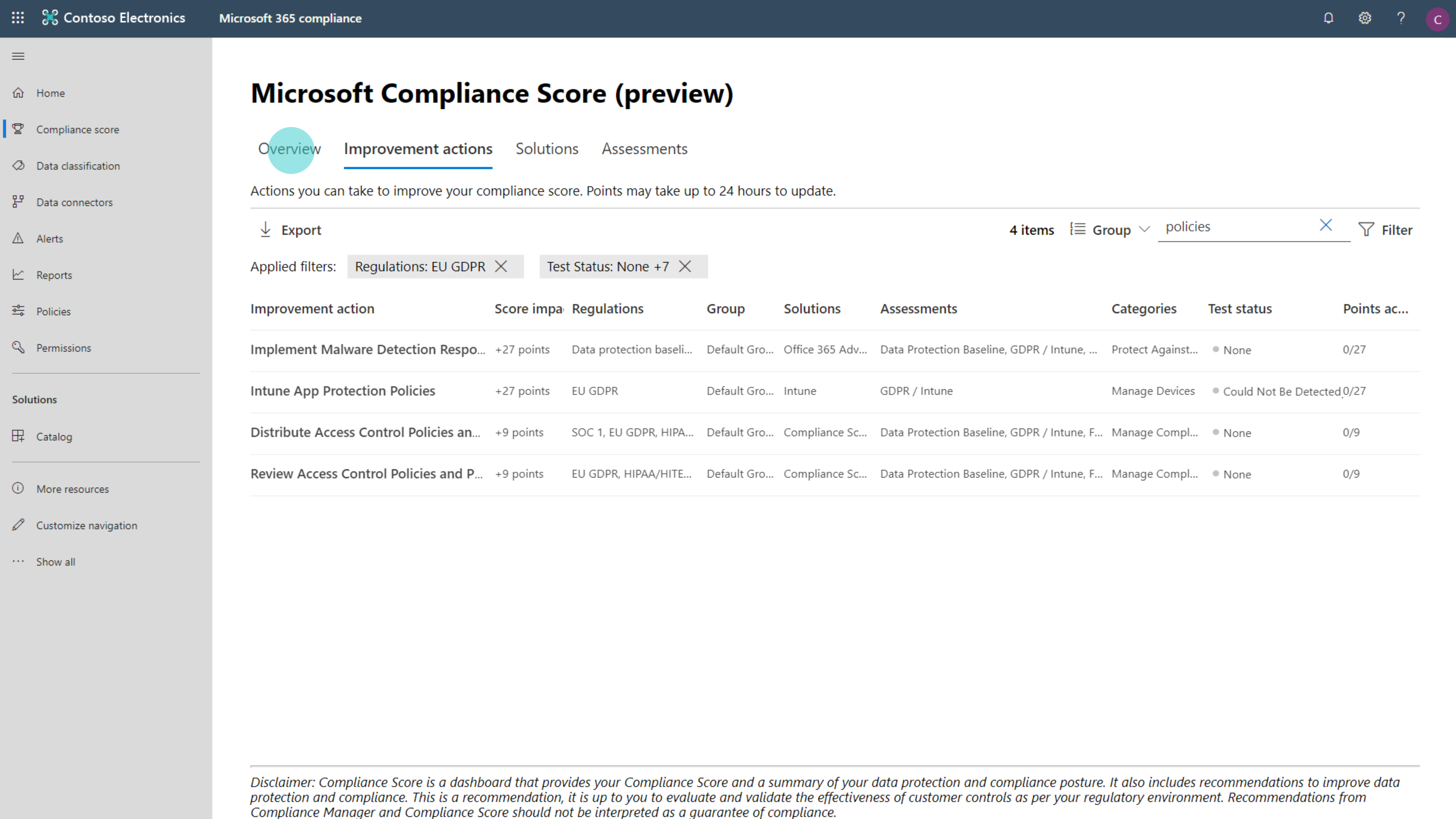
Test notes

Tested and signed off policies working as expected.

Edit test notes

Additional notes

Edit additional notes



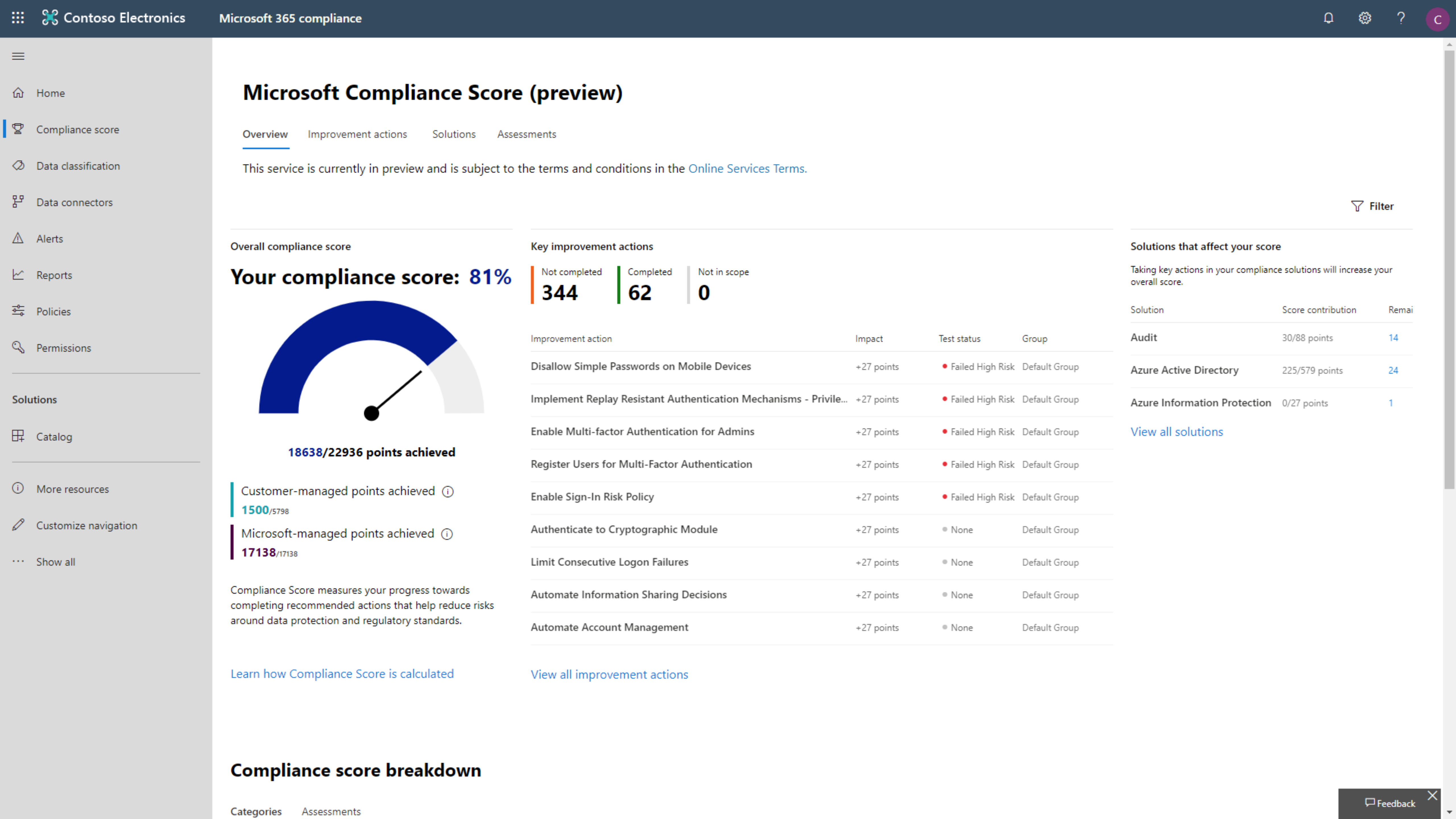
Microsoft Compliance Score (preview)

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

Applied filters: Regulations: EU GDPR ✕ Test Status: None +7 ✕

Improvement action	Score impa	Regulations	Group	Solutions	Assessments	Categories	Test status	Points ac...
Implement Malware Detection Respo...	+27 points	Data protection baseli...	Default Gro...	Office 365 Adv...	Data Protection Baseline, GDPR / Intune, ...	Protect Against...	● None	0/27
Intune App Protection Policies	+27 points	EU GDPR	Default Gro...	Intune	GDPR / Intune	Manage Devices	● Could Not Be Detected	0/27
Distribute Access Control Policies an...	+9 points	SOC 1, EU GDPR, HIPA...	Default Gro...	Compliance Sc...	Data Protection Baseline, GDPR / Intune, F...	Manage Compl...	● None	0/9
Review Access Control Policies and P...	+9 points	EU GDPR, HIPAA/HITE...	Default Gro...	Compliance Sc...	Data Protection Baseline, GDPR / Intune, F...	Manage Compl...	● None	0/9

Disclaimer: Compliance Score is a dashboard that provides your Compliance Score and a summary of your data protection and compliance posture. It also includes recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a guarantee of compliance.



Microsoft Compliance Score (preview)

Overview Improvement actions Solutions Assessments

This service is currently in preview and is subject to the terms and conditions in the Online Services Terms.

Filter

Overall compliance score

Your compliance score: 81%

18638/22936 points achieved

Customer-managed points achieved
1500/5798

Microsoft-managed points achieved
17138/17138

Compliance Score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Learn how Compliance Score is calculated

Key improvement actions

Not completed	Completed	Not in scope
344	62	0

Improvement action	Impact	Test status	Group
Disallow Simple Passwords on Mobile Devices	+27 points	● Failed High Risk	Default Group
Implement Replay Resistant Authentication Mechanisms - Privile...	+27 points	● Failed High Risk	Default Group
Enable Multi-factor Authentication for Admins	+27 points	● Failed High Risk	Default Group
Register Users for Multi-Factor Authentication	+27 points	● Failed High Risk	Default Group
Enable Sign-In Risk Policy	+27 points	● Failed High Risk	Default Group
Authenticate to Cryptographic Module	+27 points	● None	Default Group
Limit Consecutive Logon Failures	+27 points	● None	Default Group
Automate Information Sharing Decisions	+27 points	● None	Default Group
Automate Account Management	+27 points	● None	Default Group

View all improvement actions

Solutions that affect your score

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

Solution	Score contribution	Remai
Audit	30/88 points	14
Azure Active Directory	225/579 points	24
Azure Information Protection	0/27 points	1

View all solutions

Compliance score breakdown

Categories Assessments

Caveats for Compliance Score & Compliance Manager

- Compliance Manager **provides recommendations** for organizations; it doesn’t guarantee any outcome

- Recommendations from Compliance Manager **should not be interpreted as a guarantee of compliance**

- Compliance Manager gives organizations tools and information to perform **self-assessment**

- **Customers are responsible for evaluating and validating** the effectiveness of customer controls as per their regulatory environment

Microsoft

Resources & What's Next

- Visit Microsoft 365 Compliance Center at https://compliance.microsoft.com/
- Visit Compliance Manager at https://aks.ms/ComplianceManager
- Visit Service Trust Portal at https://aka.ms/stp
- Check out the video Microsoft 365 Compliance Center
- Check out the document on Microsoft 365 compliance center
- STP and CM white paper at https://aka.ms/cmwhitepaper