THAILAND Cyber Security

Microsoft Security

Cloud

SECURITY

Intensive

3 Compliance

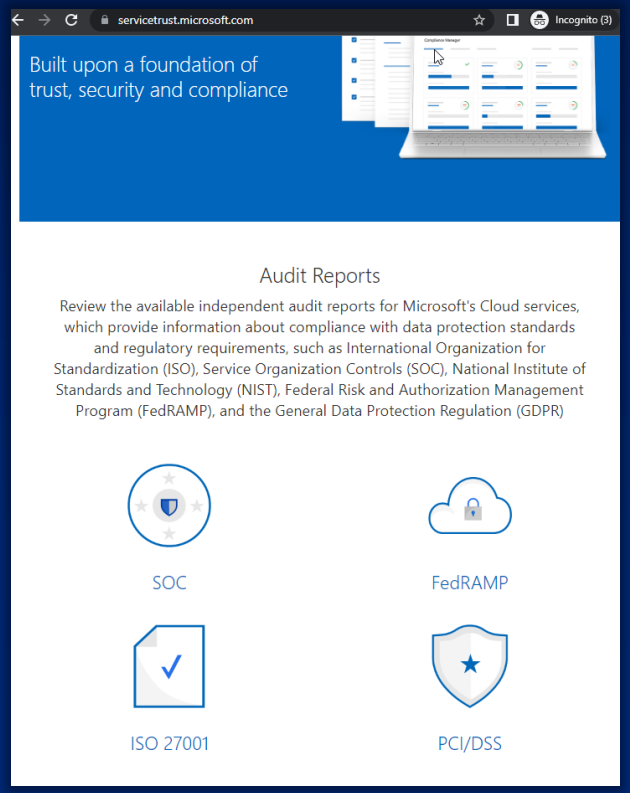
Standard Compliance
Labeling and DLP
MDE

SC-900

SECURITY
COMPLIANCE
IDENTITY

Service Trust Portal

- Show that MS comply with standards
- How MS manage privacy, compliance, security



servicetrust.microsoft.com

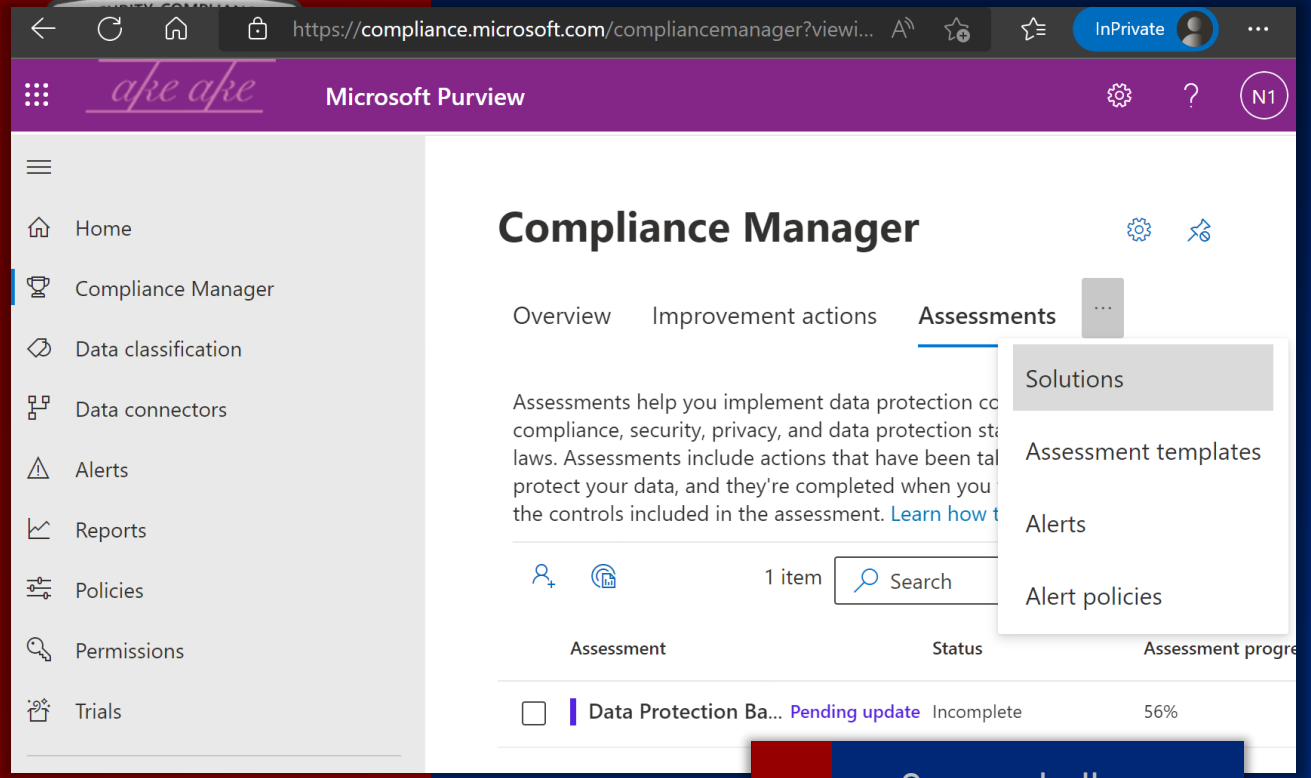
SC-900

SECURITY
COMPLIANCE
IDENTITY

Microsoft CERTIFIED

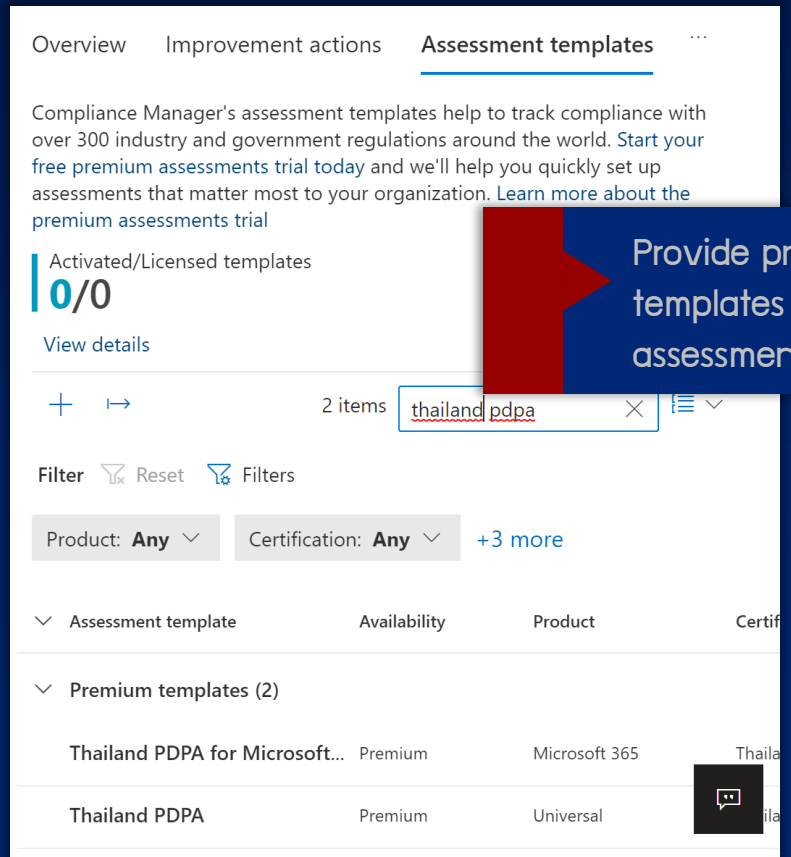
Compliance Manager

Assess compliance data **continually**



Assess whether data adhere to specific std.

compliance.microsoft.com/compliancemanager



Provide predefined templates for assessments

THCS

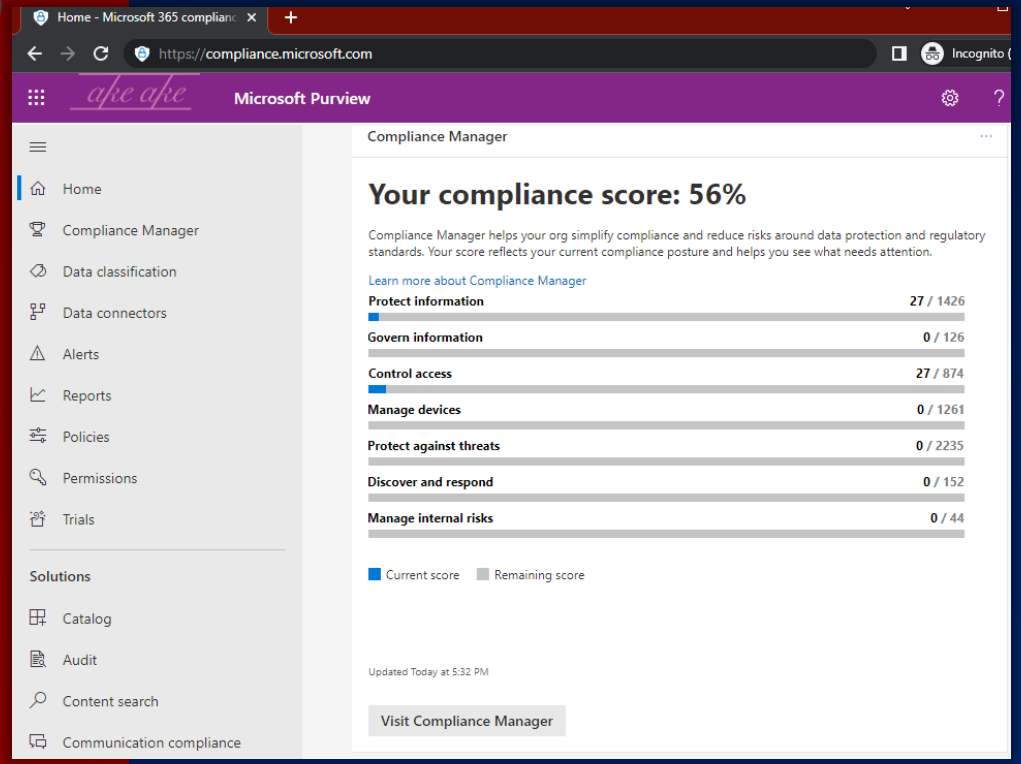
SC-900

SECURITY
COMPLIANCE
IDENTITY

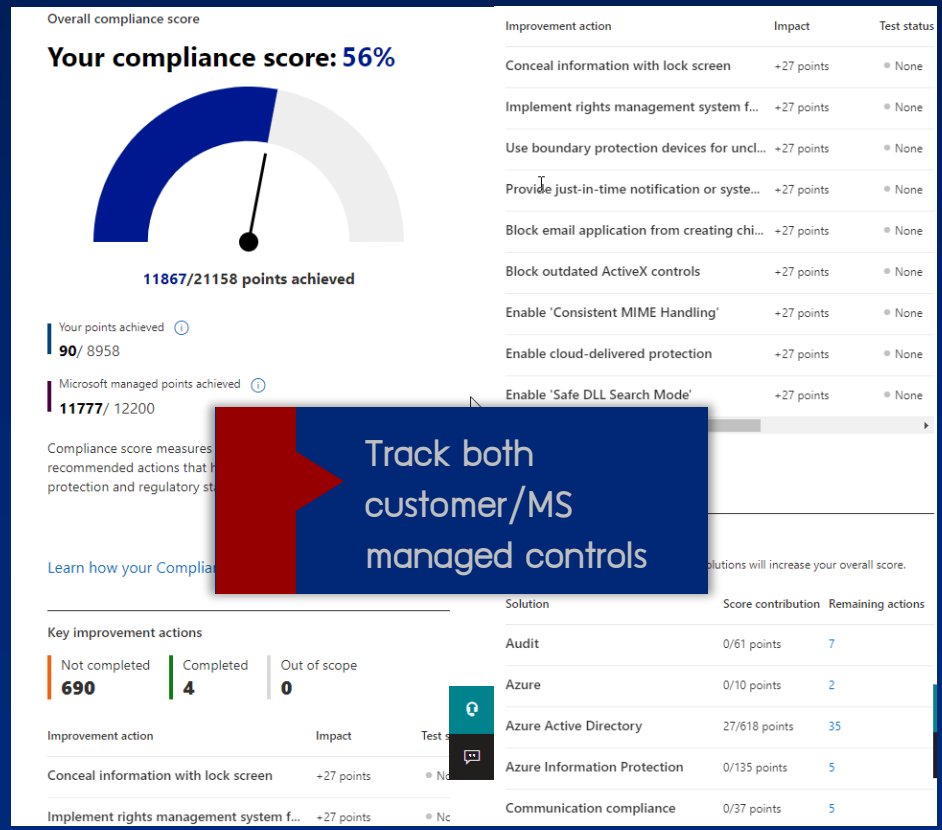
Microsoft CERTIFIED
SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS

Compliance Score

For **Data Protection** and complying **Regulation Standard**



compliance.microsoft.com/compliancemanager



THCS

SC-900

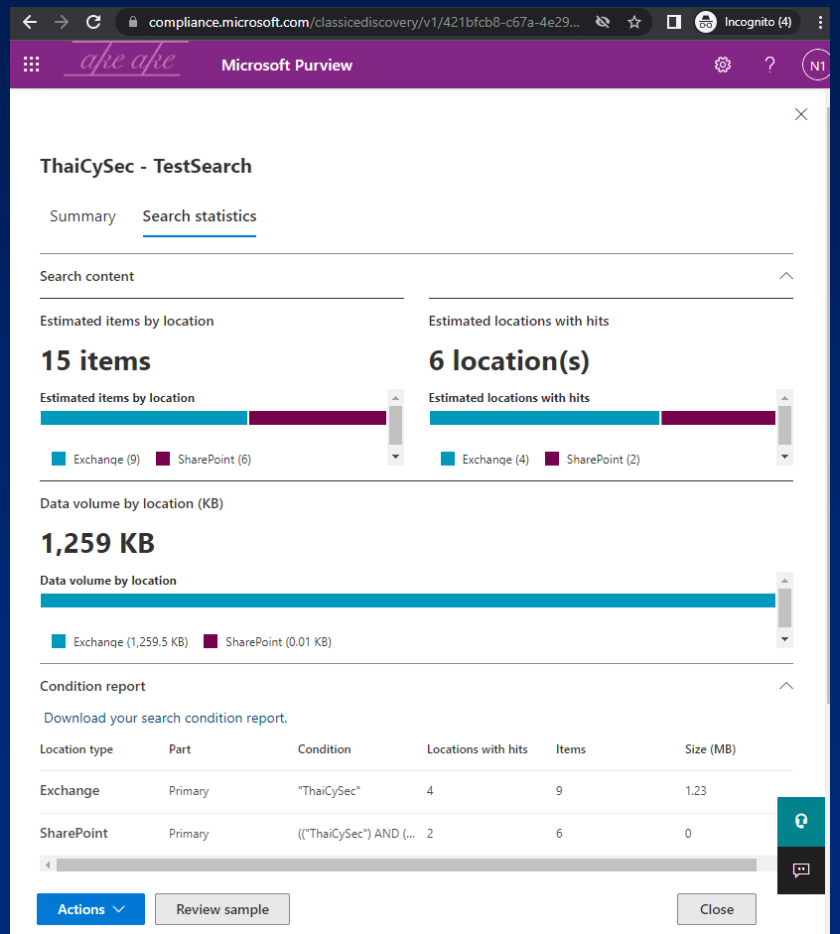
SECURITY
COMPLIANCE
IDENTITY

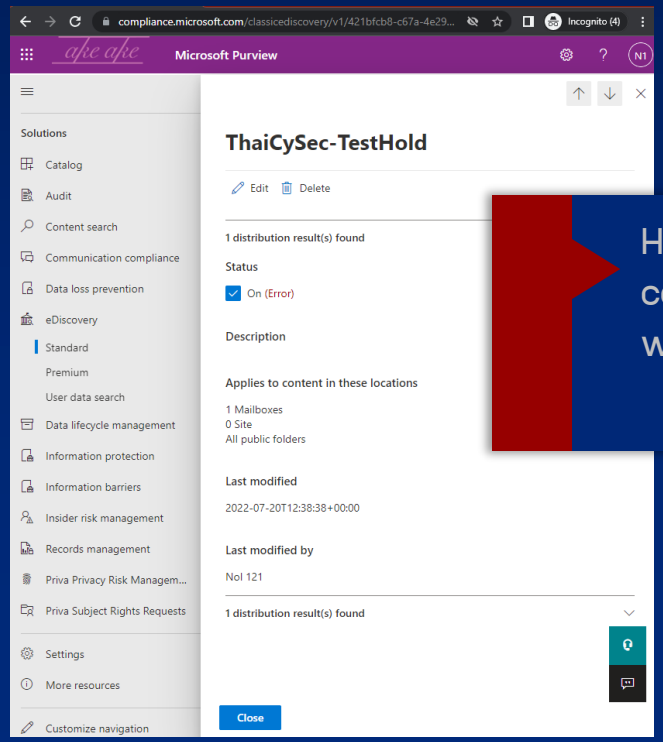
Microsoft CERTIFIED
SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS

eDiscovery — Identity / Hold data for Investigation

compliance.microsoft.com/classicediscovery

compliance.microsoft.com/advanceediscovery





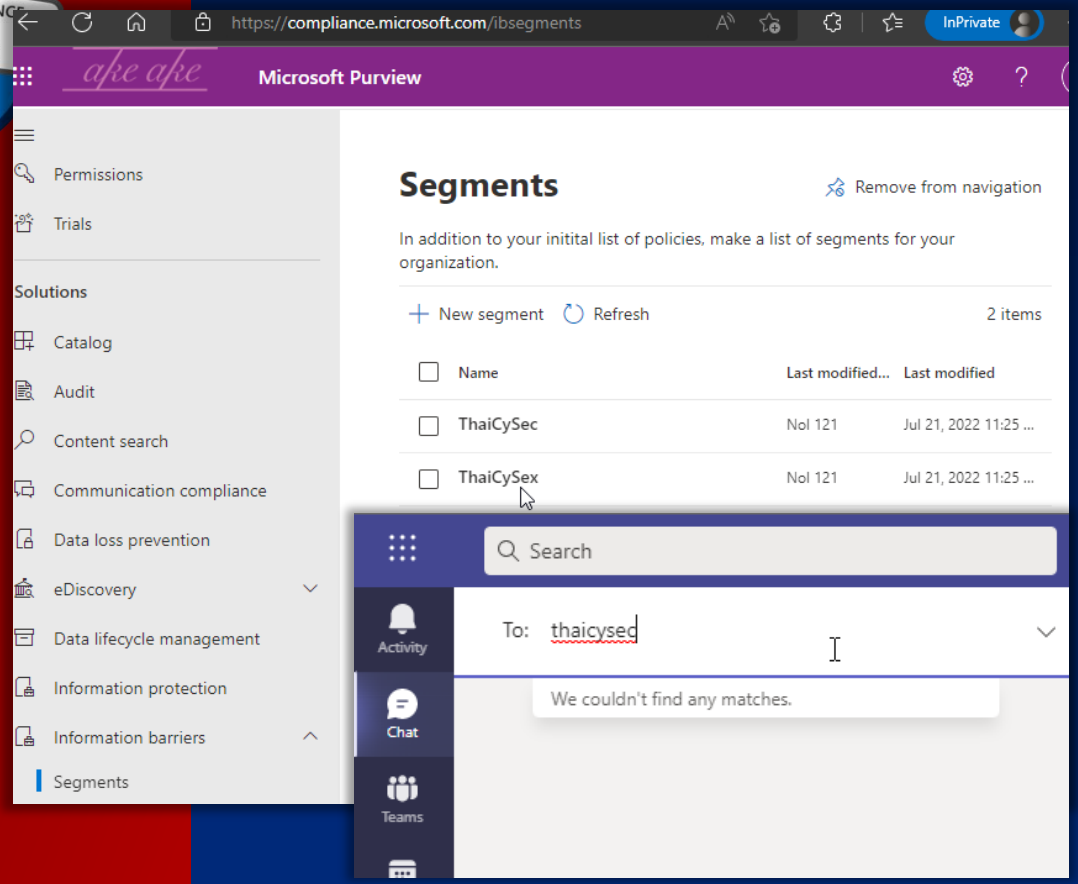
Hold before you can search content within

SC-900

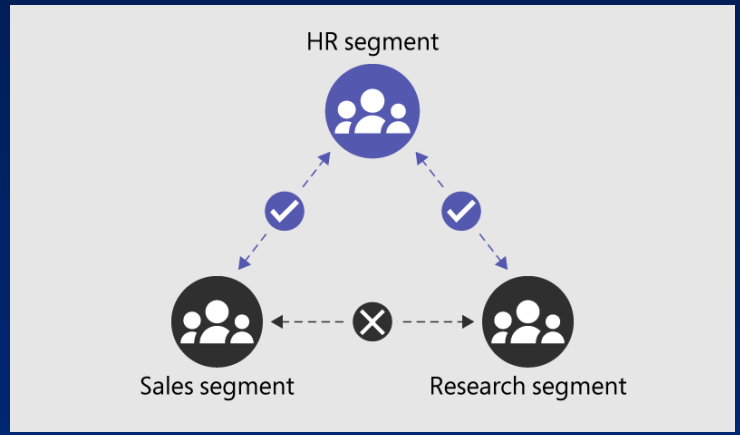
SECURITY
COMPLIANCE
IDENTITY

Information Barrier

Restrict communication via team/ sharepoint/onedrive between two department



compliance.microsoft.com/ibsegments



Not include email

SC-900

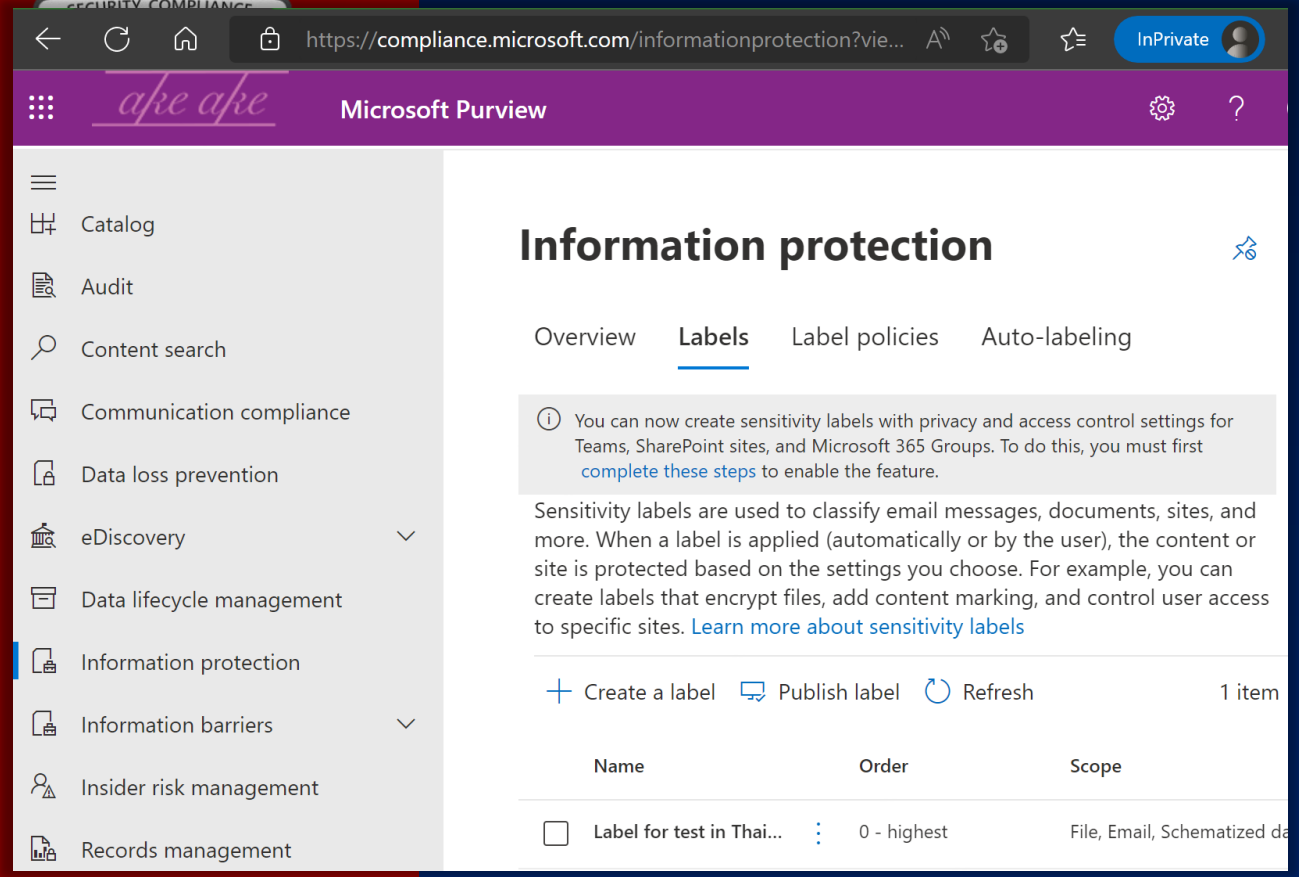
SECURITY
COMPLIANCE
IDENTITY

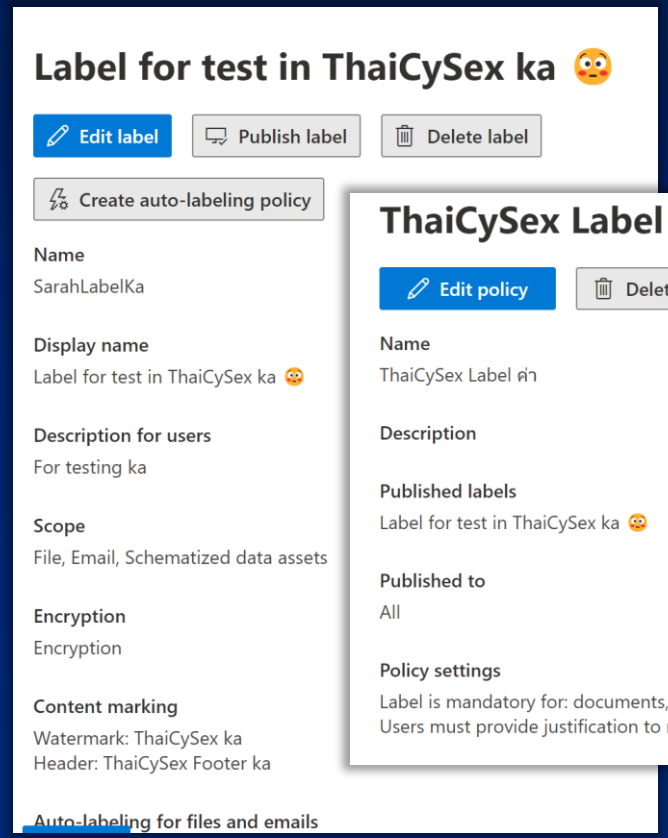
Information Protection

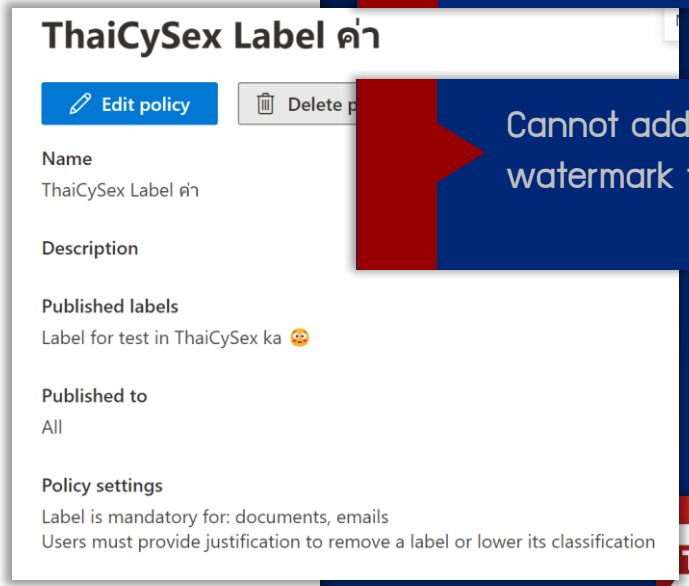
Protect sensitive data from being exposed to unauthorized users

Use **sensitivity label/policy**

compliance.microsoft.com/informationprotection







Determine which watermark add to files

Cannot add watermark to email!

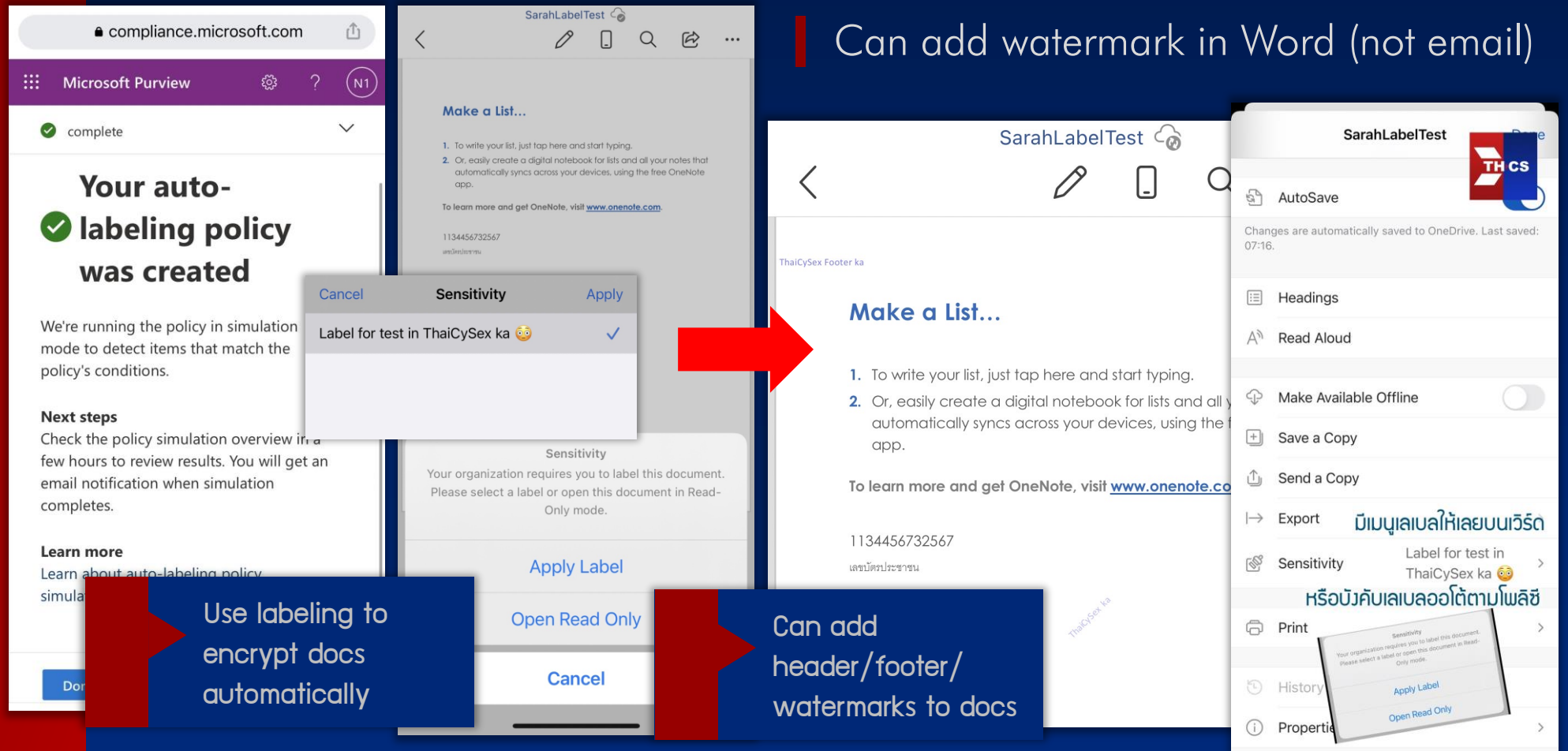
SC-900

SECURITY
COMPLIANCE
IDENTITY

Microsoft CERTIFIED
SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS

Information Protection

- User can apply label manually
- One file, One label
- Can add watermark in Word (not email)



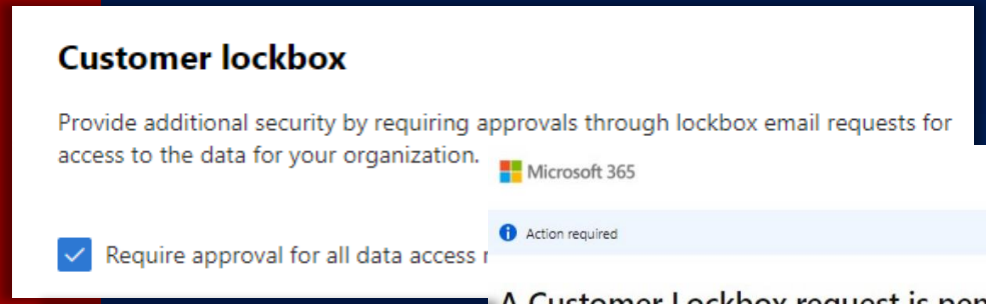
SC-900

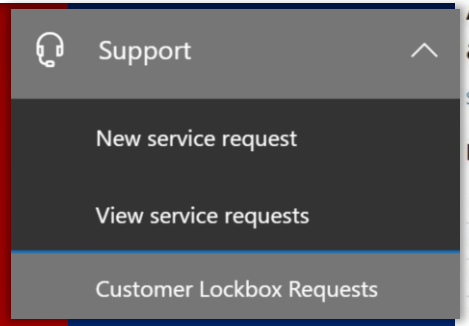
SECURITY
COMPLIANCE
IDENTITY

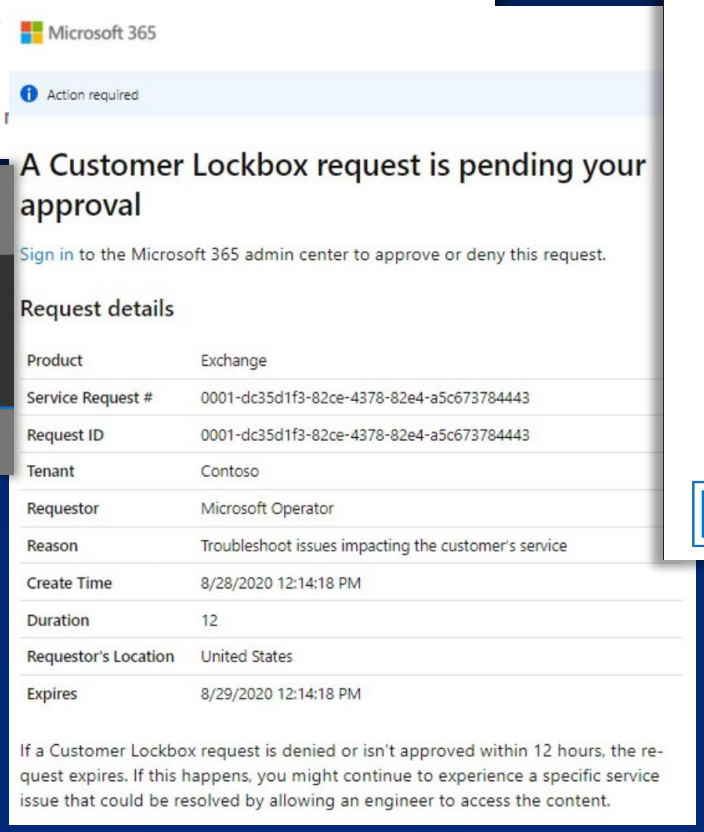
Microsoft CERTIFIED
SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS

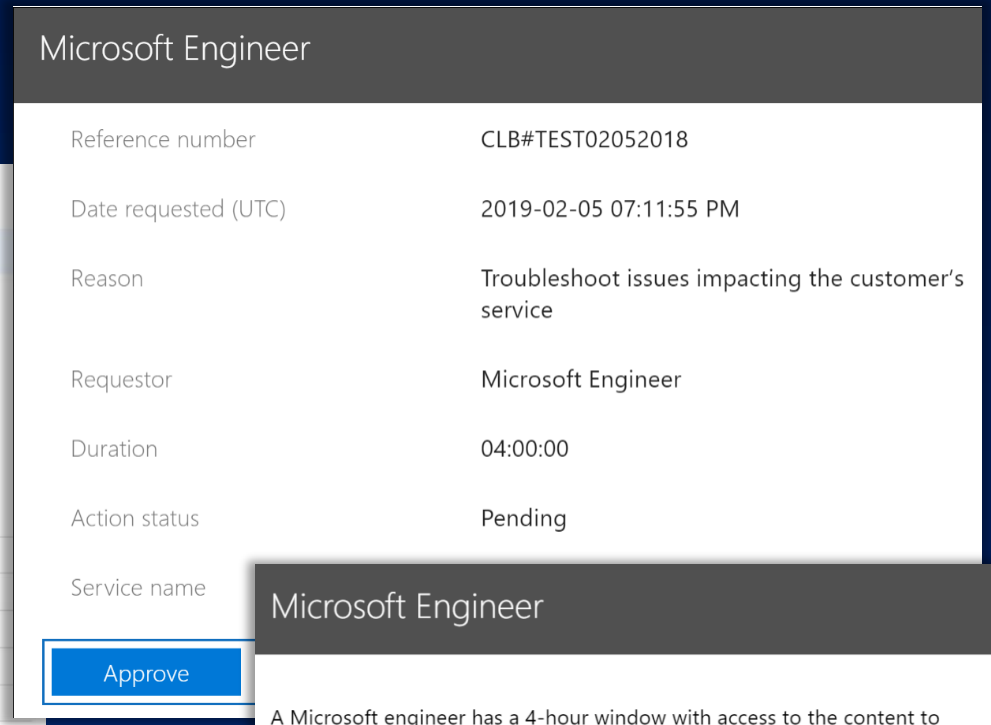
Customer Lockbox

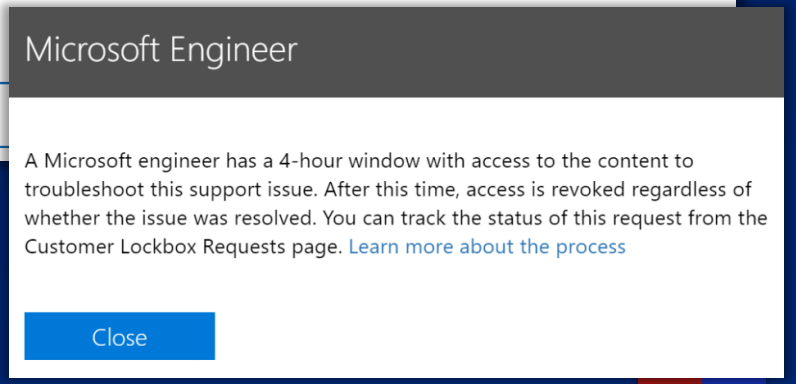
Provide MS engineer to access data in Exchange/Sharepoint/OneDrive









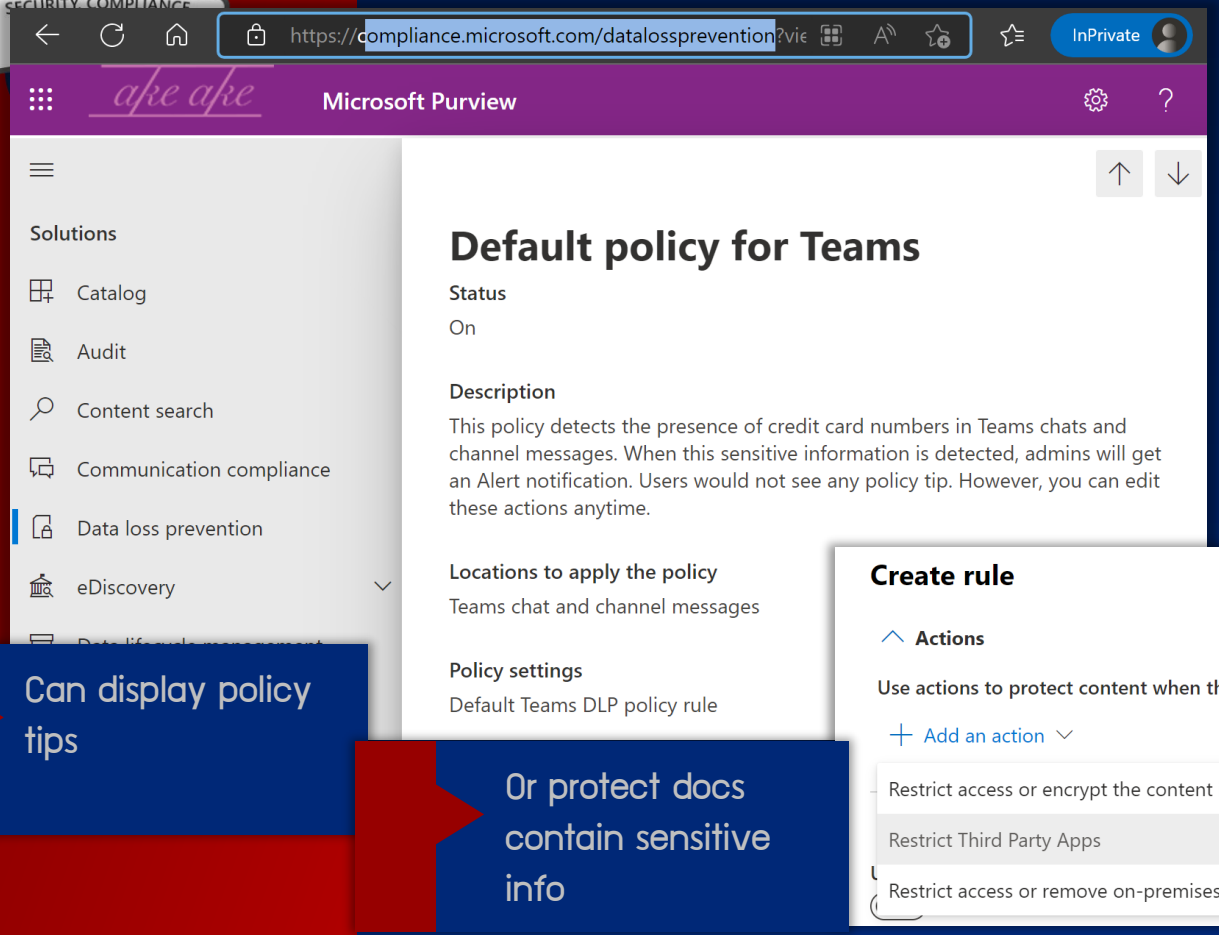


SC-900

SECURITY
COMPLIANCE
IDENTITY

Data Loss Prevention (DLP)

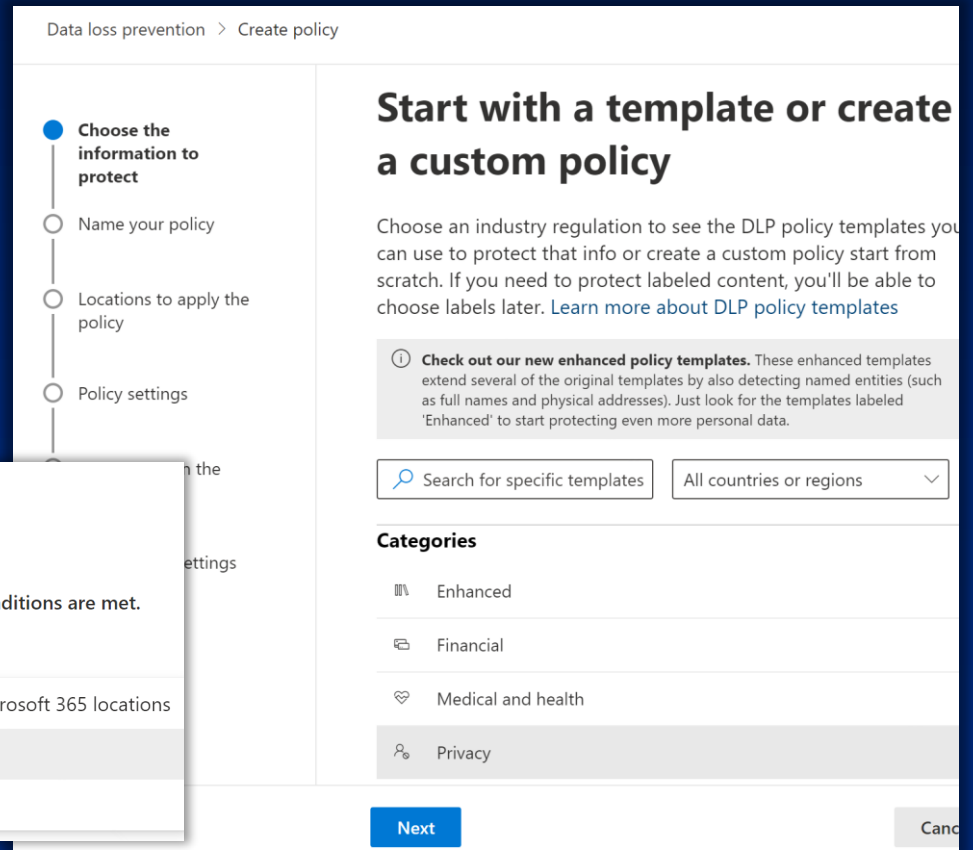
Restrict sending emails contain sensitive data e.g. customer lists, credit card no.



Can display policy tips

Or protect docs contain sensitive info

compliance.microsoft.com/datalossprevention



SC-900

SECURITY
COMPLIANCE
IDENTITY

Insider Risk

"insider" risks such as data leak from employee, IP theft, fraud, insider trading, confidentiality violation etc.

Categories

- Data theft
- Data leaks
- Security policy violations (preview)
- Health record misuse (preview)

Templates

- Data theft by departing users

Categories

- Data theft
- Data leaks
- …review)
- …iew)

Templates

- General data leaks
- Data leaks by priority users
- Data leaks by disgruntled users (preview)

Many new template to find bad bad guys in your office

Categories

- Data theft
- Data leaks
- Security policy violations (preview)
- Health record misuse (preview)

Templates

- General security policy violations (preview)
- Security policy violations by departing users (preview)
- Security policy violations by disgruntled users (preview)
- Security policy violations by priority users (preview)

Templates

- General health record misuse (preview)

General health record misuse (preview)

Detects health record misuse by a user included in this policy. Misus can range from accessing privileg patient records to accessing recor of patients from family or neighb

THCS

SC-900

SECURITY
COMPLIANCE
IDENTITY

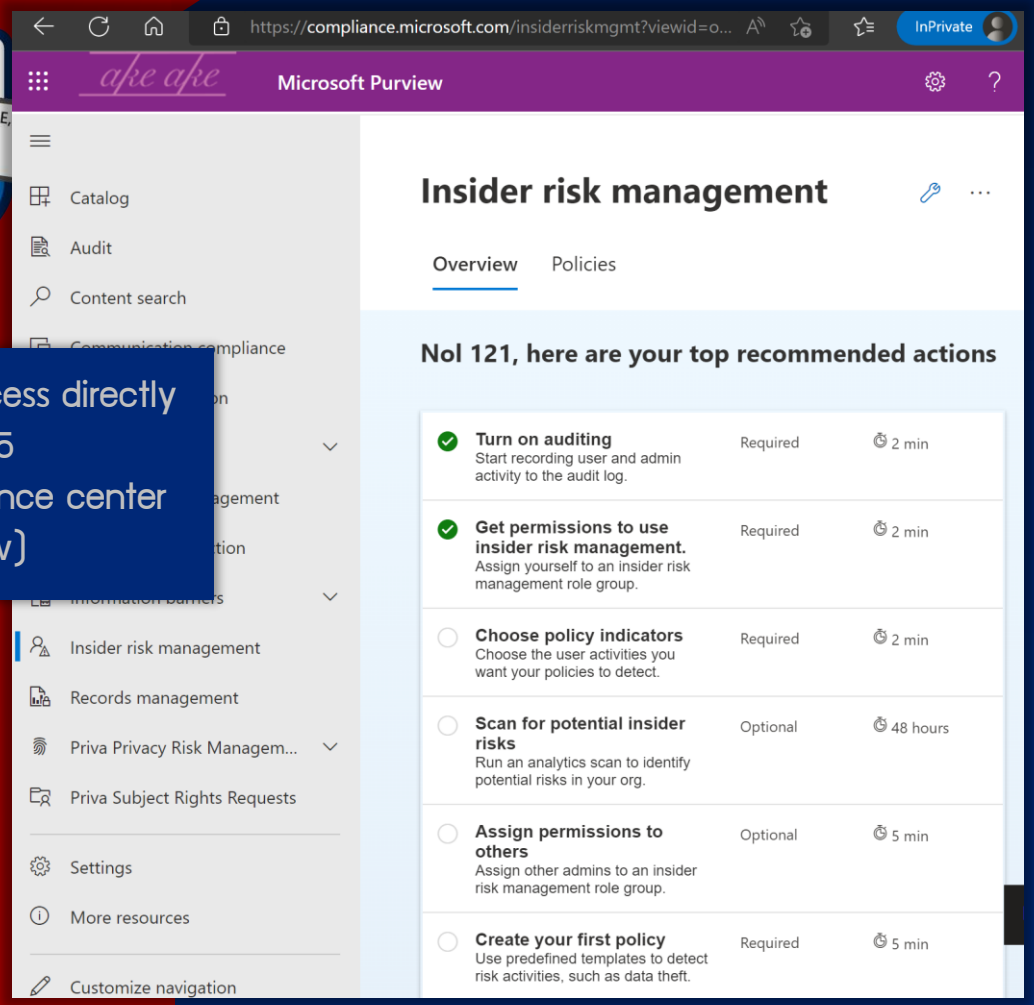
Phishing is not "insider" risks

Insider Risk

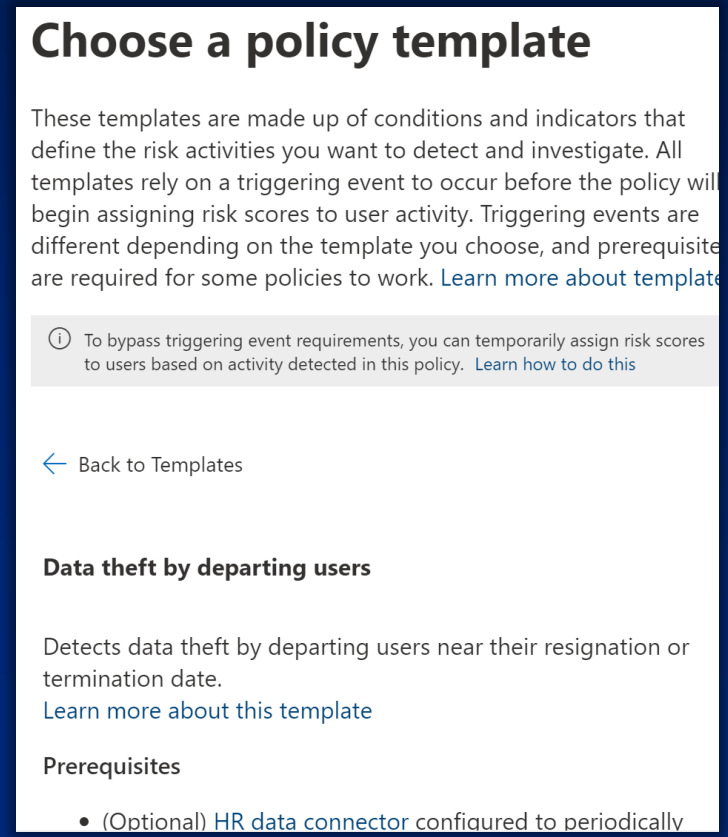
"insider" risks such as data leak from employee, IP theft, fraud, insider trading, confidentiality violation etc.

Microsoft CERTIFIED
SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS

Can access directly from 365 Compliance center (Purview)



compliance.microsoft.com/insiderriskmgmt



THCS

SC-900

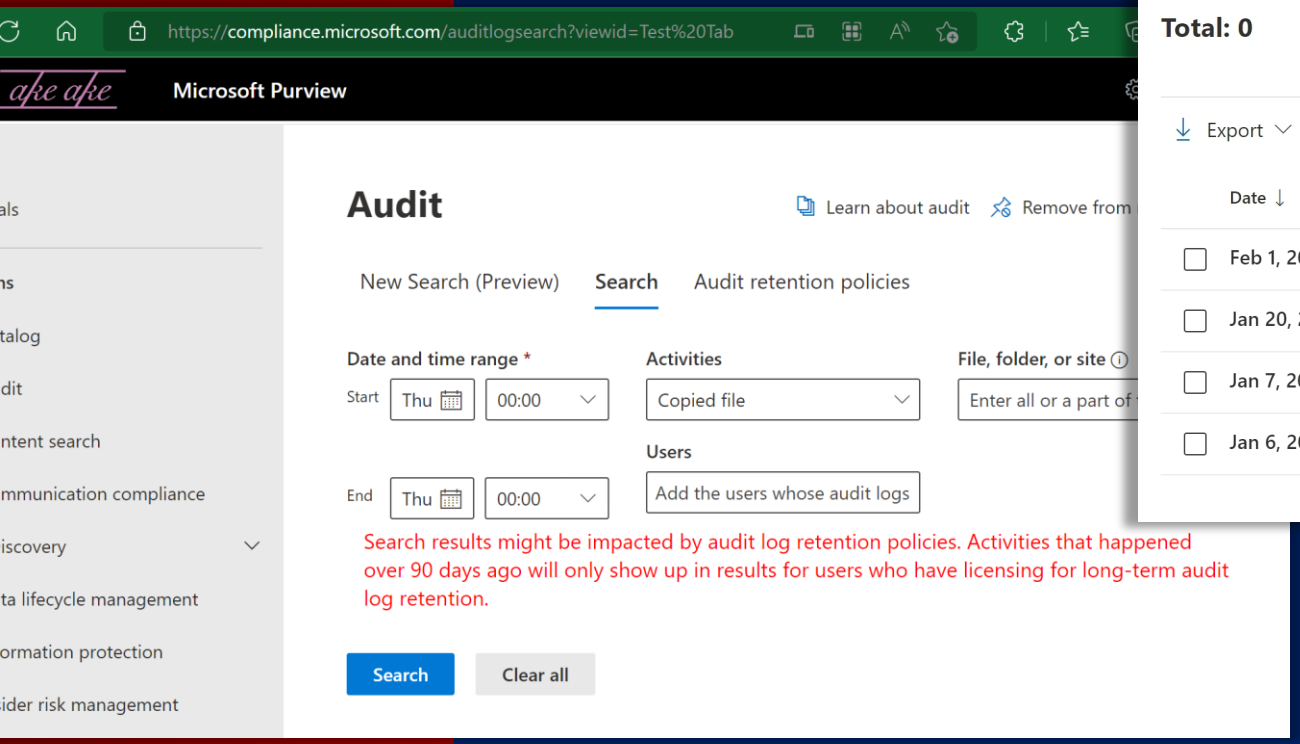
SECURITY
COMPLIANCE
IDENTITY

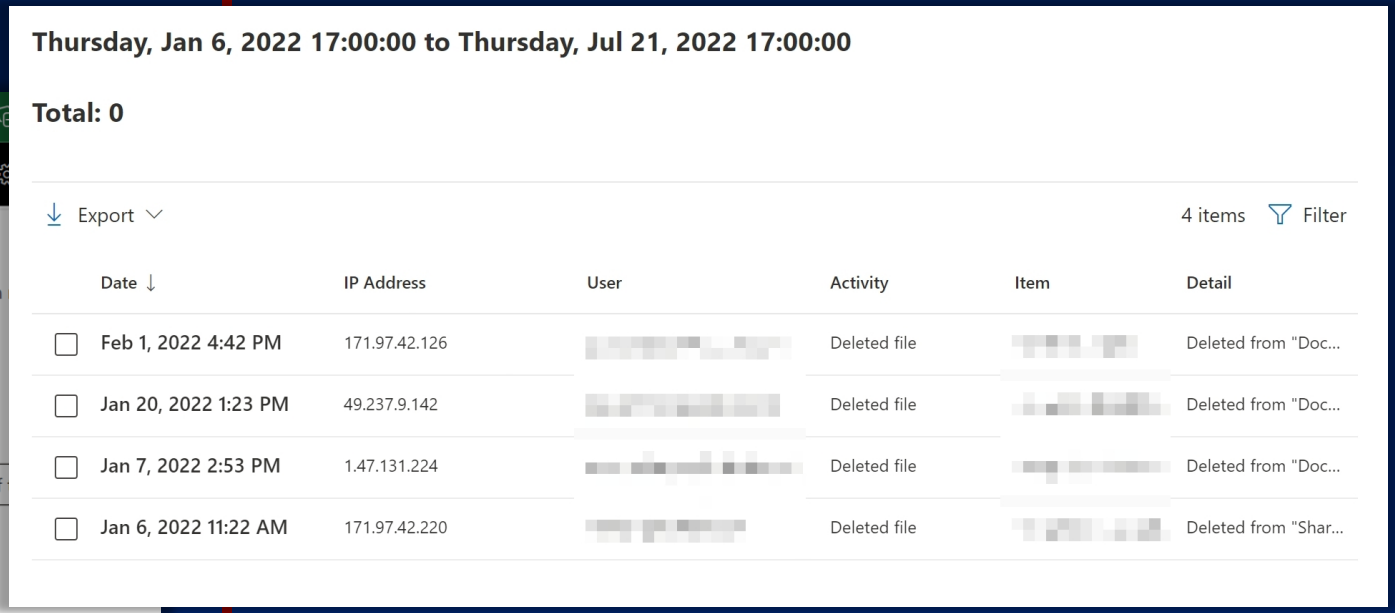
(Basic) Audit

License: M365 E3

- Audit user activities
- Retain logs for 90 days

compliance.microsoft.com/auditlogsearch





Thursday, Jan 6, 2022 17:00:00 to Thursday, Jul 21, 2022 17:00:00

Total: 0

Export
4 items
Filter

Date	IP Address	User	Activity	Item	Detail
Feb 1, 2022 4:42 PM	171.97.42.126		Deleted file		Deleted from "Doc...
Jan 20, 2022 1:23 PM	49.237.9.142		Deleted file		Deleted from "Doc...
Jan 7, 2022 2:53 PM	1.47.131.224		Deleted file		Deleted from "Doc...
Jan 6, 2022 11:22 AM	171.97.42.220		Deleted file		Deleted from "Shar...

SC-900

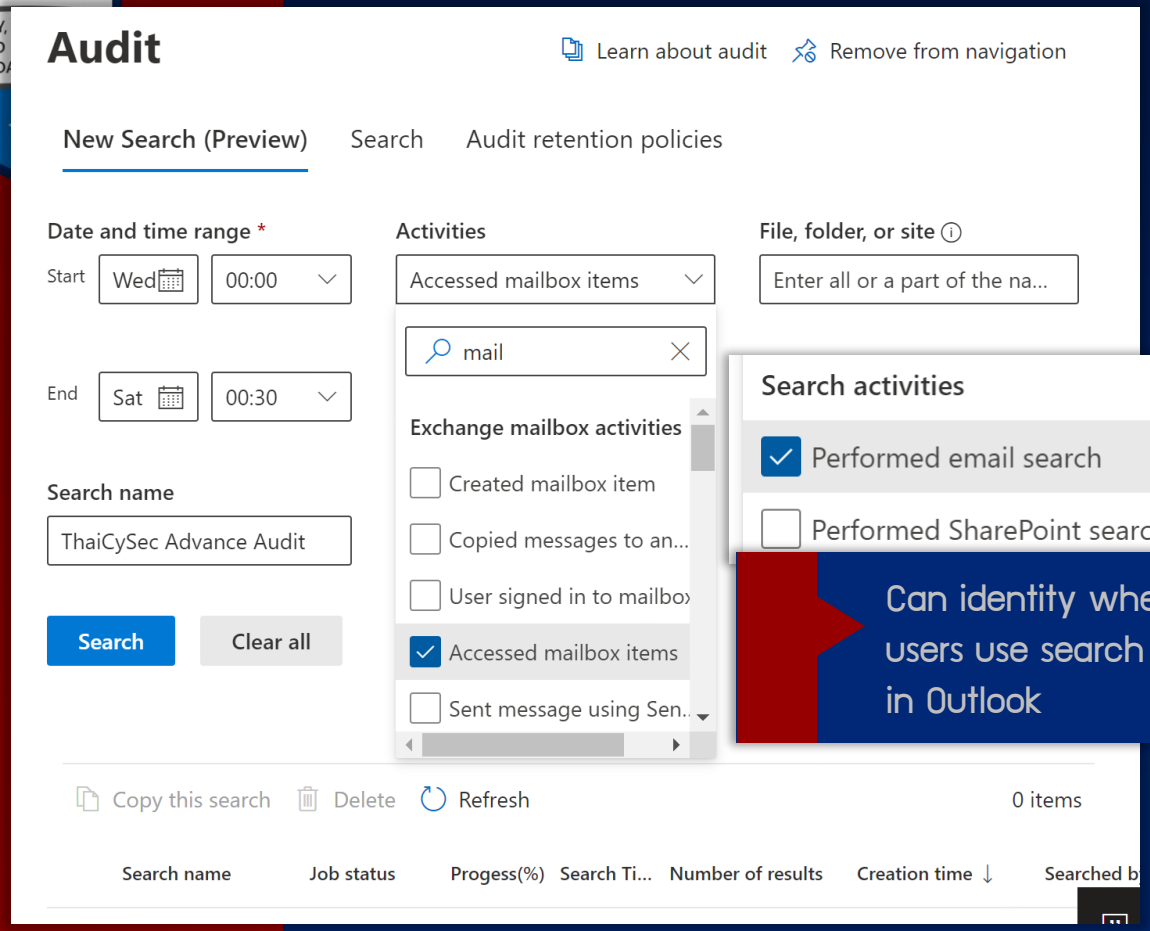
SECURITY
COMPLIANCE
IDENTITY

Purview Audit (Premium) (E5)

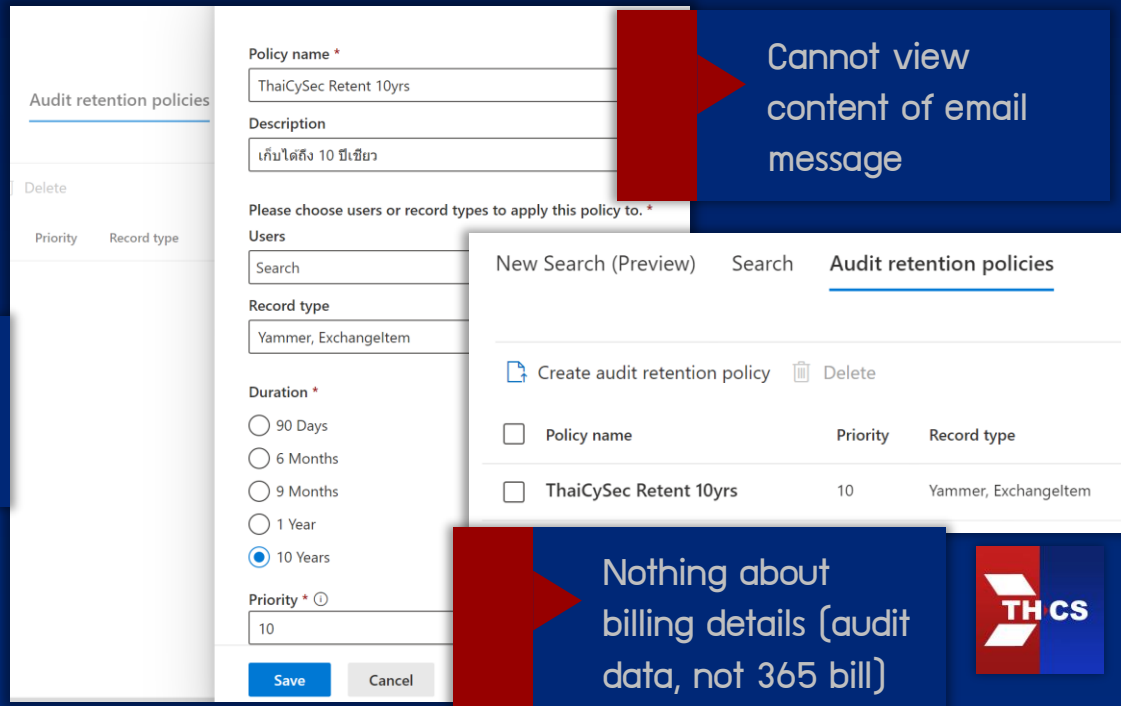
Advance Audit

- Retain up to 10 years
- More events: MailItemsAccessed
- Customer-dedicate bandwidth

compliance.microsoft.com/auditlogsearch



Can identity when users use search bar in Outlook



Cannot view content of email message

Nothing about billing details (audit data, not 365 bill)

SC-900

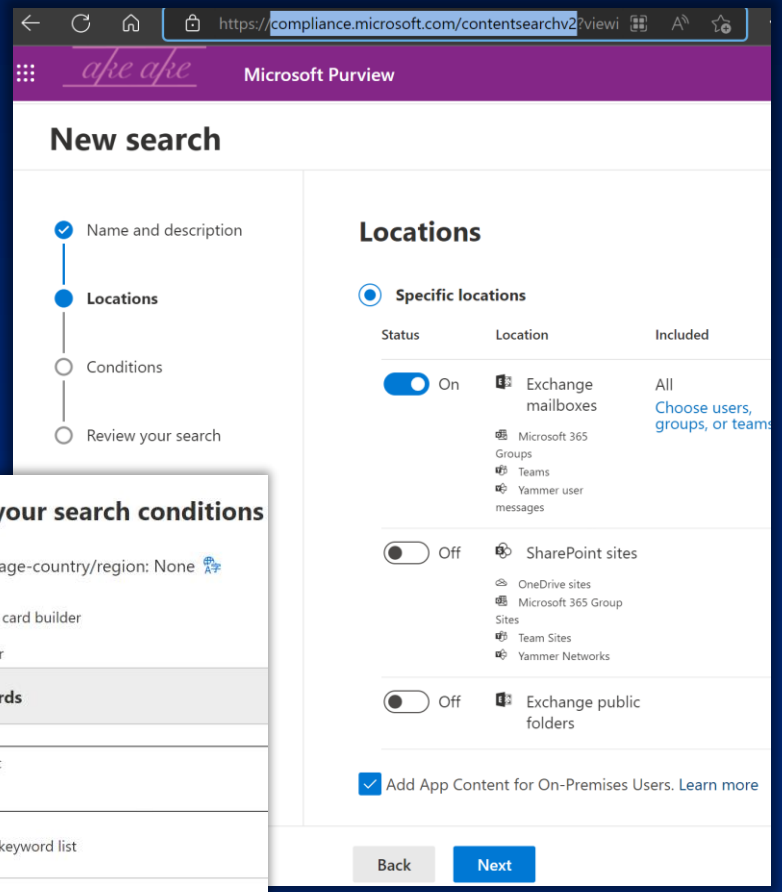
SECURITY
COMPLIANCE
IDENTITY

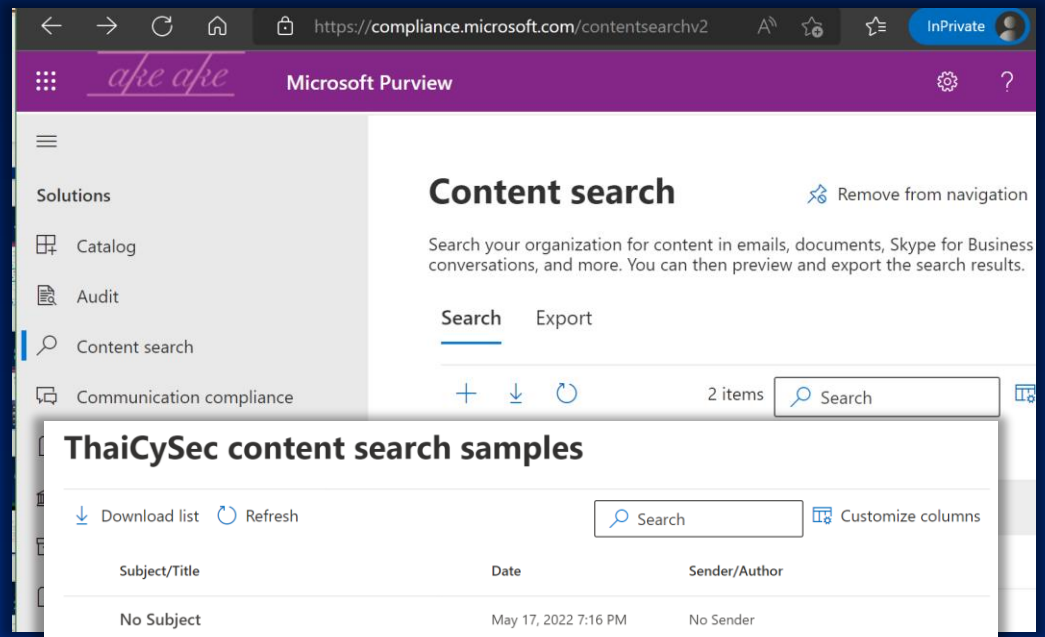
Microsoft CERTIFIED
SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS

Content Search

Identify docs in Email/Sharepoint contain keywords

compliance.microsoft.com/contentsearchv2





THCS

SC-900

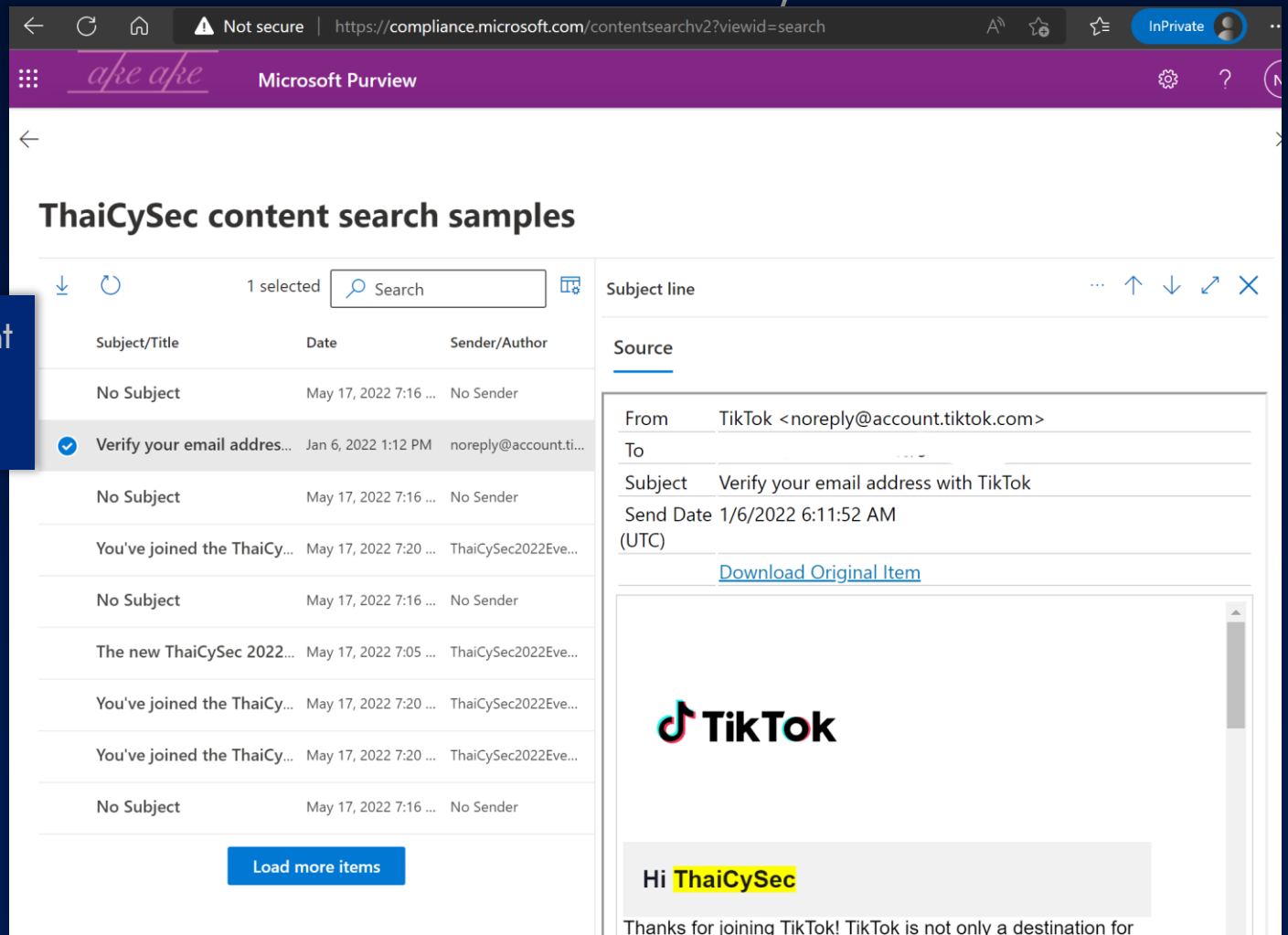
SECURITY
COMPLIANCE
IDENTITY

Microsoft CERTIFIED
SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS

Content Search

Identify docs in Email/Sharepoint contain keywords

Can see full content or even download them



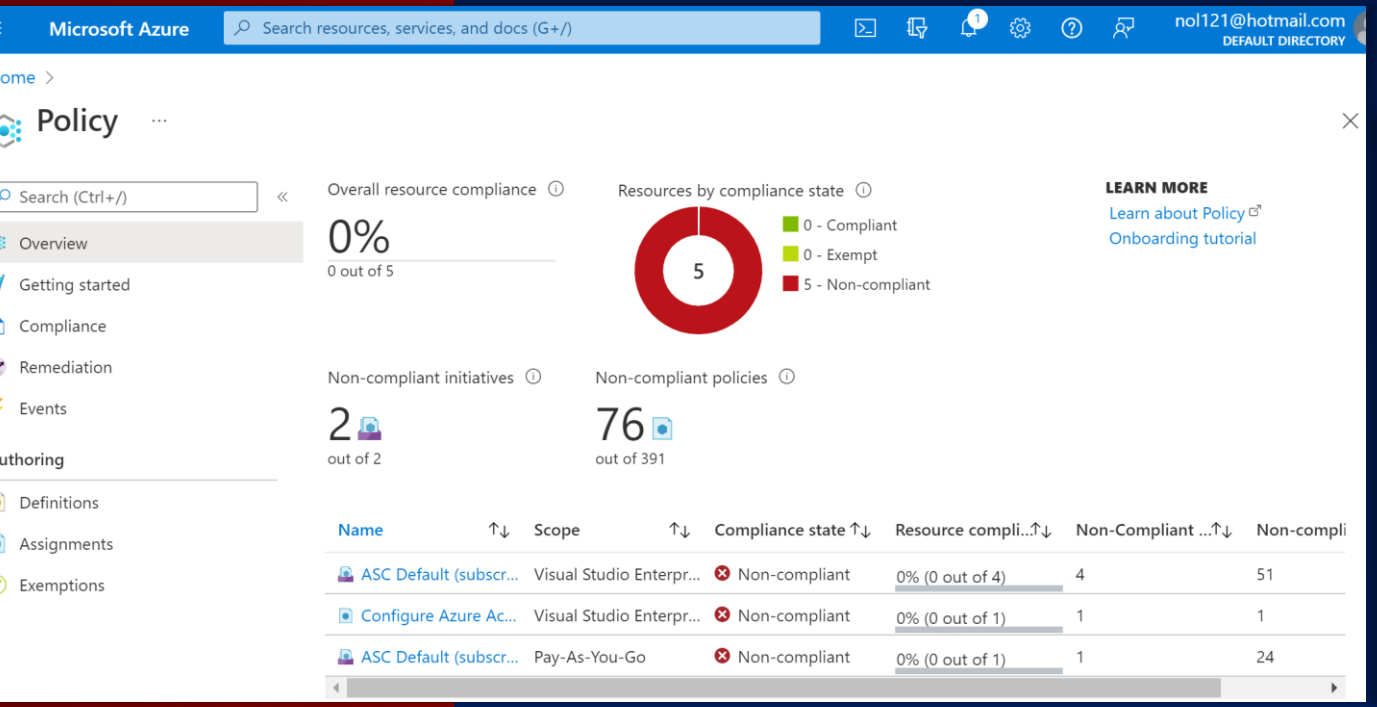
SC-900

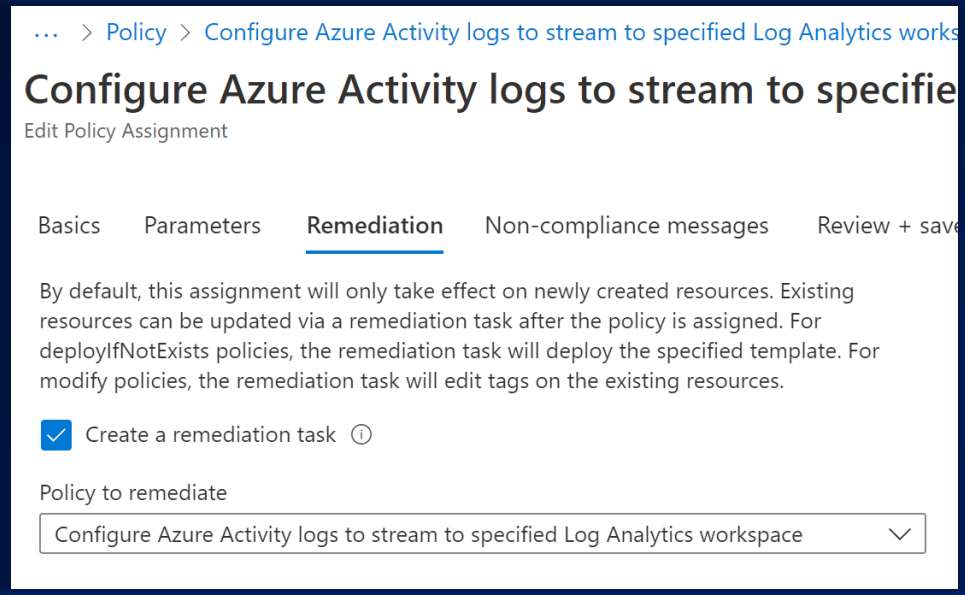
SECURITY
COMPLIANCE
IDENTITY

Microsoft CERTIFIED
SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS

Azure Policy

- Ensure resources comply standard
- Automatic remediation
- Evaluate when create/update resource/assigned policy/per 24hrs cycle



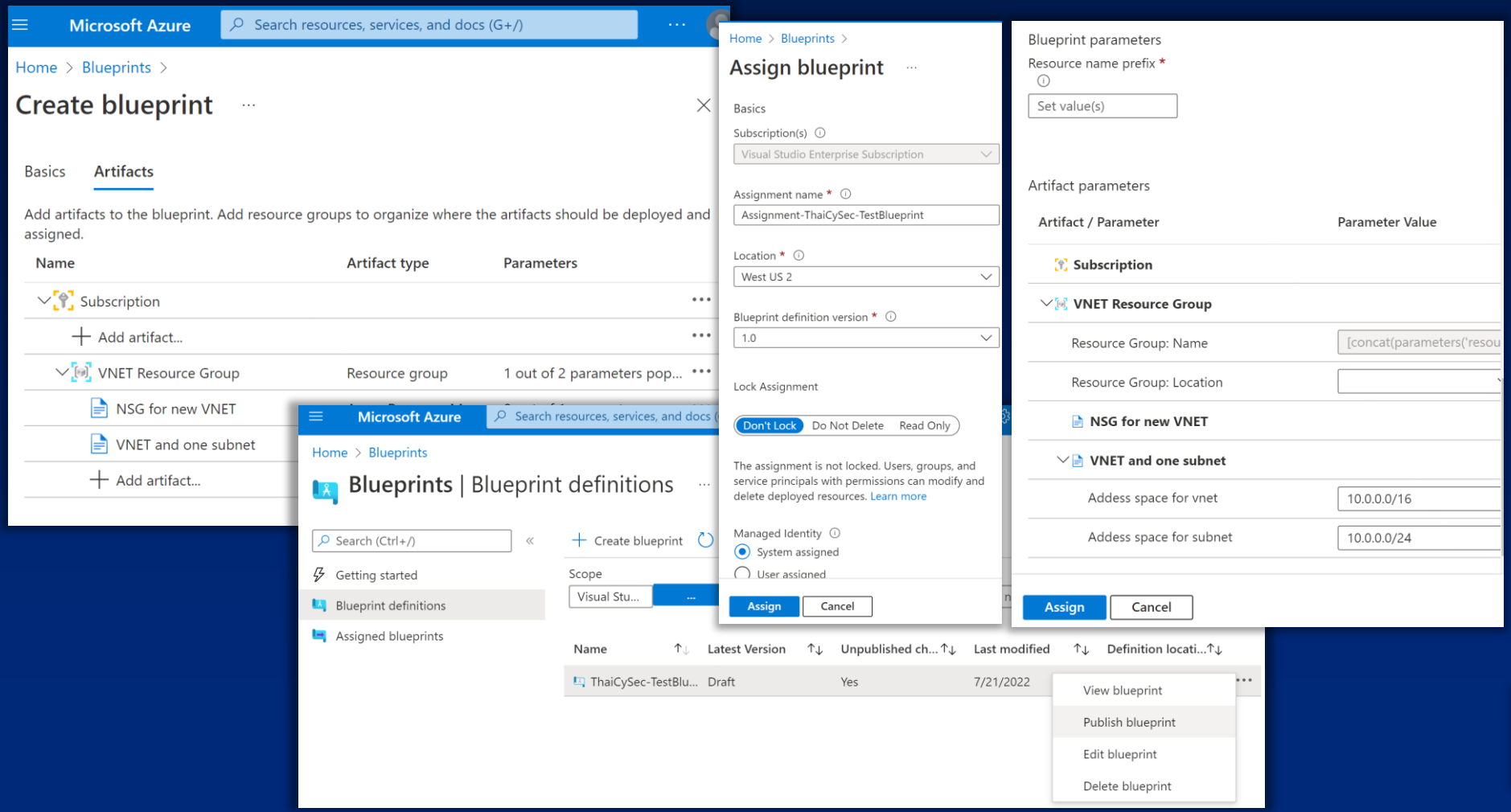


SC-900

SECURITY
COMPLIANCE
IDENTITY

Microsoft CERTIFIED
SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS

Azure Blueprint — Provision resources across subscriptions in consistent manner

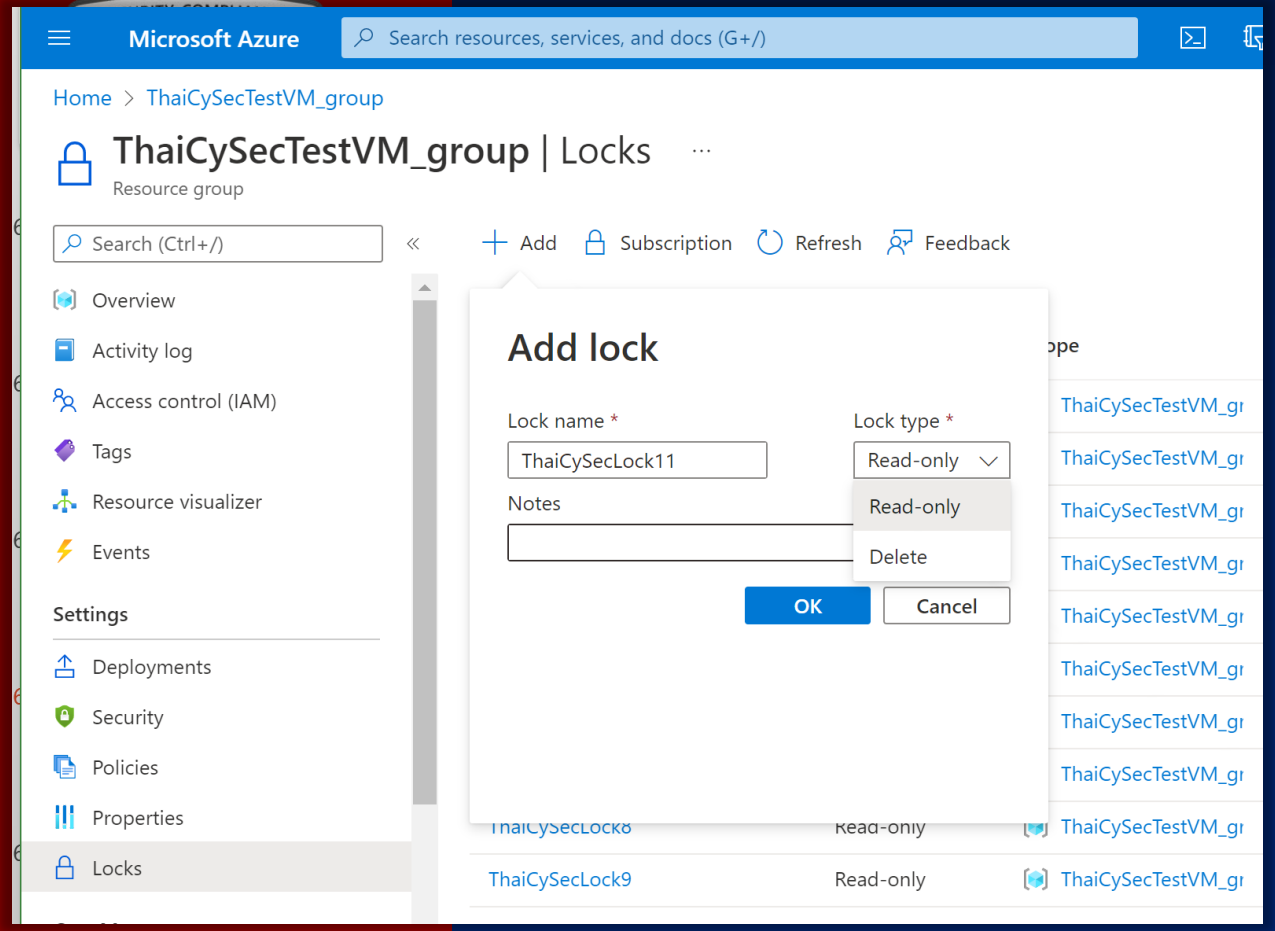


SC-900

SECURITY
COMPLIANCE
IDENTITY

Microsoft CERTIFIED

Resource Lock



- Apply Lock to resources/RG/ or even subscription
- Protect from accidental delete or modification
- One resource can be applied many locks
- Cannot be partially delete, e.g. cannot delete RG that has delete-lock resource within

THCS

Exam Example in SC-900

Purview Compliance

Which specific feature can auto encrypt document based on specific conditions?

A. Retention Label/Policy
B. Sensitivity Label/Policy
C. Data Loss Prevention (DLP)
D. Azure Information Protection (AIP)
E. Purview Governance

Answer: **Sensitivity Label**

Hint: We can set such as “Confidential” label with (auto) labeling policy that which docs get this label, encrypt them.

Exam Example in SC-900

Purview Compliance

About Sensitivity Label:

1. Can add custom watermark to Word documents? Yes/No
2. Can add custom watermark to Email? Yes/No
3. Can add custom header/footer to documents? Yes/No
4. Can use for encrypting documents? Yes/No

Answer: **Y/N/Y/Y**

Hint: No any way/feature in this world that can add watermark in typical email.

Exam Example in SC-900

Purview Compliance

How frequent the Compliance Manager assess compliance data for organization?

A. Weekly
B. Monthly
C. On-Demand only
D. Continually

Answer: **Continually**
Hint: such as when open docs/email or has any change in each docs.

Exam Example in SC-900

Purview Compliance

To prevent two groups/departments sharing/collaborating info, we use:

A. Data Loss Prevention (DLP)
B. Insider Risk
C. Sensitivity Label
D. eDiscovery Hold
E. Customer Lockbox
F. Information Barrier

Answer: **Information Barrier**
Hint: as barrier in Teams/SharePoint

Exam Example in SC-900

Purview Compliance

To prevent employee sending mail contains sensitive info like costing sheet, ID no, credit card info, we use:

A. Data Loss Prevention (DLP)
B. Insider Risk
C. Sensitivity Label
D. eDiscovery Hold
E. Customer Lockbox
F. Information Barrier

Answer: **DLP**
Hint: Data **Loss =** Loss to **outside**; DLP for **email** message/attached docs

Exam Example in SC-900

Purview Compliance

Purview (365) Compliance Information Protection (Sensitivity Label) is used for?

A. Prevent Password Leak
B. Prevent unwanted communication via Teams and SharePoint
C. Prevent mailing specific info to outside of organization
D. Prevent exposing sensitive data to unauthorized users
E. Protect information from malware

Answer: **Protect sensitive data from being exposed**

Hint: Information Protection = **Sensitivity** Policies = Protect **sensitive** data from exposed even to unwanted users inside the organization.

Exam Example in SC-900

Purview Compliance

When Microsoft Engineer would like to access customer's data for solving support tickets, they would request us to approve which feature to scope only necessary they need to access in Exchange/SharePoint/OneDrive ?

A. eDiscovery
B. Litigation Hold
C. Data Lost Prevention (DLP)
D. Customer Lockbox
E. Live Support

Answer: **Customer Lockbox**
Hint: Lockbox = Sandbox for Microsoft Engineer in our system

Exam Example in SC-900

Purview Compliance

About Insider Risk:

1. You can manage Insider Risk from M365 (Purview) Compliance portal Yes/No
2. You can access Insider Risk management at security.microsoft.com portal Yes/No
3. Phishing is one Insider Risk you can manage Yes/No
4. Data Breach from unhappy employee is one Insider Risk you can manage Yes/No

Answer: **Y/N/N/Y**

Hint: **Insider** means people inside org. such as employee.
Insider Risk is **Compliance** feature, on compliance.microsoft.com

Exam Example in SC-900

Purview Compliance

About Compliance Manager:

1. Have many predefined Compliance template to use Yes/No
2. Can check how much you comply with variety of standards Yes/No
3. Can check compliance with Thailand PDPA Yes/No
4. Cannot track controls that Microsoft-side manage Yes/No

Answer: **Y/Y/Y/N**

Hint: **Compliance manager** feature is for compliance checking with many standards, with many templates. So, of course, must track both customer and Microsoft system side.

Exam Example in SC-900

Azure Features

Which feature in Azure letting you implement/update resources across subscriptions in consistent manner?

A. Azure Policy
B. Azure Resource Manager Template
C. Azure Blueprint
D. Azure DevOps
E. Azure Function

Answer: **Azure Blueprint**

Hint: “across subscriptions (at once)”. ARM templates can be artifacts in one Blueprint, but template is just template, just data that other features use such Blueprint.