

A graphic element on the left side of the slide features a stylized map of Thailand. The map is composed of several overlapping triangles in shades of red, blue, and grey, creating a layered effect. The word "THAILAND" is overlaid on this graphic in large, white, sans-serif capital letters.

THAILAND

Cyber  
Security



 Microsoft Security

# Cloud SECURITY Intensive





# Compliance

Standard Compliance  
Labeling and DLP

MDE A blue icon showing a monitor and a smartphone connected by a line, representing mobile device integration.

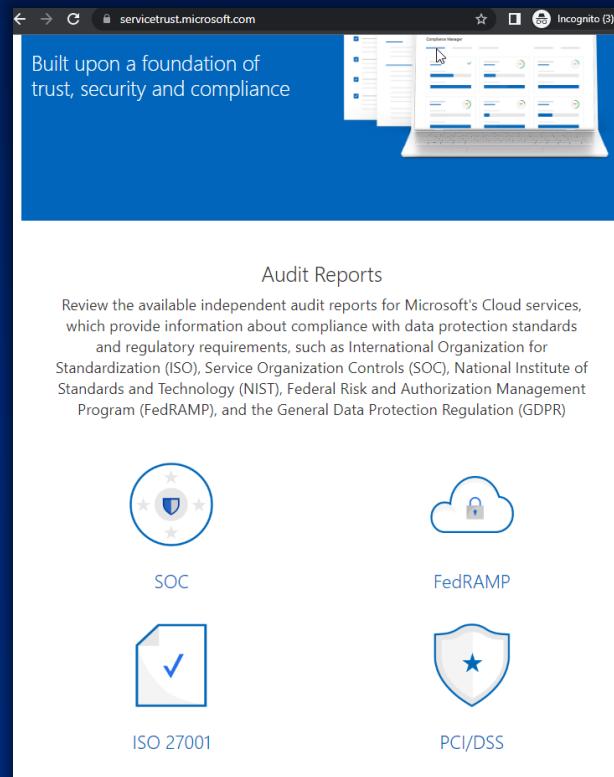


# SC-900

SECURITY  
COMPLIANCE  
IDENTITY



## Service Trust Portal



The screenshot shows a web browser displaying the Service Trust Portal at [servicetrust.microsoft.com](http://servicetrust.microsoft.com). The page has a blue header bar with the text "Built upon a foundation of trust, security and compliance". Below the header, there's a section titled "Audit Reports" with a detailed description of available independent audit reports for Microsoft's Cloud services, mentioning ISO, SOC, NIST, FedRAMP, and GDPR. At the bottom, there are four circular icons with labels: SOC (with a shield icon), ISO 27001 (with a checkmark icon), FedRAMP (with a cloud and lock icon), and PCI/DSS (with a shield icon).

Show that MS comply with standards

How MS manage privacy,  
compliance, security

[servicetrust.microsoft.com](http://servicetrust.microsoft.com)



# SC-900

SECURITY  
COMPLIANCE  
IDENTITY

## Compliance Manager

Assess compliance data continually

The screenshot shows the Microsoft Purview Compliance Manager interface. On the left, there's a navigation bar with links like Home, Compliance Manager, Data classification, Data connectors, Alerts, Reports, Policies, Permissions, and Trials. The main area has a title 'Compliance Manager' and tabs for Overview, Improvement actions, and Assessments (which is selected). Below this, there's a section about Assessments and a table with one item: 'Data Protection Ba...' (Pending update, Incomplete, 56%). A callout box at the bottom right says 'Assess whether data adhere to specific std.'.

The screenshot shows the 'Assessment templates' page in Compliance Manager. It features a header with tabs for Overview, Improvement actions, and Assessment templates (selected). A callout box on the right says 'Provide predefined templates for assessments'. Below the tabs, there's a section for 'Activated/Licensed templates' showing '0/0' and a 'View details' button. There's also a search bar containing 'thailand pdpa'. A 'Filter' section with dropdowns for Product (Any) and Certification (Any) is shown. The main table lists two items: 'Thailand PDPA for Microsoft...' (Premium, Microsoft 365, Thailand) and 'Thailand PDPA' (Premium, Universal, Thailand). A THCS logo is in the bottom right corner.

# SC-900

SECURITY  
COMPLIANCE  
IDENTITY



## Compliance Score

The screenshot shows the Microsoft Purview Compliance Manager dashboard. At the top, it displays "Your compliance score: 56%". Below this, a list of categories with their current and total scores: Protect information (27 / 1426), Govern information (0 / 126), Control access (27 / 874), Manage devices (0 / 1261), Protect against threats (0 / 2235), Discover and respond (0 / 152), and Manage internal risks (0 / 44). A legend indicates that blue bars represent the "Current score" and grey bars represent the "Remaining score". The bottom of the page includes a "Visit Compliance Manager" button and a note that the data was updated "Today at 5:32 PM".

For Data Protection and  
complying Regulation Standard

[compliance.microsoft.com/compliancemanager](https://compliance.microsoft.com/compliancemanager)

The screenshot shows the Microsoft Compliance Manager portal. It features a large circular gauge meter indicating a "Your compliance score: 56%" and "11867/21158 points achieved". Below the meter, a callout box states "Track both customer/MS managed controls". The page lists various "Improvement actions" with their impact and test status. It also shows sections for "Key improvement actions" (Not completed: 690, Completed: 4, Out of scope: 0) and "Audit" results for different services like Azure, Azure Active Directory, and Azure Information Protection. The bottom right corner features the THCS logo.



# SC-900

SECURITY  
COMPLIANCE  
IDENTITY



## eDiscovery

Identity / Hold data for Investigation

A screenshot of the Microsoft Purview eDiscovery interface. It shows search results for "ThaiCySec - TestSearch".

**Estimated items by location:**  
**15 items**  
Estimated items by location: Exchange (9) SharePoint (6)

**Estimated locations with hits:**  
**6 location(s)**  
Estimated locations with hits: Exchange (4) SharePoint (2)

**Data volume by location (KB):**  
**1,259 KB**  
Data volume by location: Exchange (1,259.5 KB) SharePoint (0.01 KB)

**Condition report:**  
Download your search condition report.

Location type	Part	Condition	Locations with hits	Items	Size (MB)
Exchange	Primary	"ThaiCySec"	4	9	1.23
SharePoint	Primary	((("ThaiCySec")) AND (...))	2	6	0

**Actions:** Actions ▾ Review sample Close

compliance.microsoft.com/classicediscovery

compliance.microsoft.com/advanceediscovery

A screenshot of the Microsoft Purview eDiscovery interface showing a "Hold" configuration.

**Solutions:** Catalog, Audit, Content search, Communication compliance, Data loss prevention, eDiscovery (Standard, Premium, User data search), Data lifecycle management, Information protection, Information barriers, Insider risk management, Records management, Priva Privacy Risk Management, Priva Subject Rights Requests, Settings, More resources.

**ThaiCySec-TestHold:**

- Edit Delete
- 1 distribution result(s) found
- Status: On (Error)
- Description
- Applies to content in these locations:  
1 Mailboxes, 0 Site, All public folders
- Last modified: 2022-07-20T12:38:38+00:00
- Last modified by: Nol 121
- 1 distribution result(s) found

**Close**

Hold before you can search content within



# SC-900

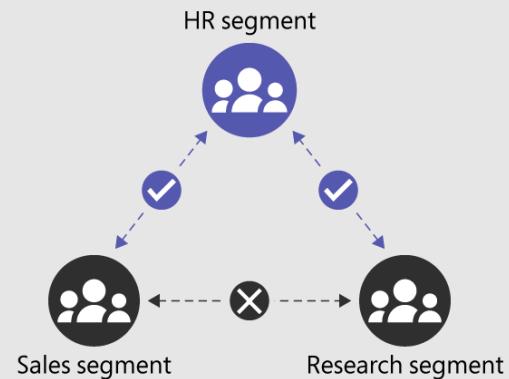
SECURITY  
COMPLIANCE  
IDENTITY

The screenshot shows the Microsoft Purview Compliance interface. On the left, a sidebar lists various compliance solutions like Permissions, Trials, Catalog, Audit, Content search, Communication compliance, Data loss prevention, eDiscovery, Data lifecycle management, Information protection, and Information barriers. A 'Segments' option is selected. The main area is titled 'Segments' and shows a list of two items: 'ThaiCySec' and 'ThaiCySex'. Below this is a search bar with 'Search' and a 'To:' field containing 'thaicysed'. A message says 'We couldn't find any matches.' At the bottom, there's a 'Teams' icon.

## 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

The screenshot shows the Microsoft Purview interface with the 'Information protection' section selected. The 'Labels' tab is active, displaying a message about creating sensitivity labels and a list of existing labels.

**Information protection**

Overview Labels Label policies Auto-labeling

You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first [complete these steps](#) to enable the feature.

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

+ Create a label Publish label Refresh 1 item

Name	Order	Scope
Label for test in Thai...	0 - highest	File, Email, Schematized data

Protect sensitive data from being exposed to unauthorized users

Use sensitivity label/policy

compliance.microsoft.com/informationprotection

### Label for test in ThaiCySex ka 😊

[Edit label](#) [Publish label](#) [Delete label](#)

[Create auto-labeling policy](#)

Name

SarahLabelKa

Display name

Label for test in ThaiCySex ka 😊

Description for users

For testing ka

Scope

File, Email, Schematized data assets

Encryption

Encryption

Content marking

Watermark: ThaiCySex ka

Header: ThaiCySex Footer ka

[Auto-labeling for files and emails](#)

Determine which watermark add to files

### ThaiCySex Label ຄ່າ

[Edit policy](#) [Delete p...](#)

Name

ThaiCySex Label ຄ່າ

Description

Published labels

Label for test in ThaiCySex ka 😊

Published to

All

Policy settings

Label is mandatory for: documents, emails

Users must provide justification to remove a label or lower its classification

Cannot add watermark to email!



# SC-900

SECURITY  
COMPLIANCE  
IDENTITY



## Information Protection

The screenshot shows a Microsoft Purview interface with a banner stating "Your auto-labeling policy was created". Below it, a message says "We're running the policy in simulation mode to detect items that match the policy's conditions." A "Next steps" section instructs to check the policy simulation overview in a few hours. A "Learn more" link is also present. A red callout box at the bottom right points to the text "Use labeling to encrypt docs automatically".

A "Sensitivity" dialog box is open, showing "Label for test in ThaiCySex ka 😊". A red arrow points from the "Apply" button in this dialog to the "Apply Label" button in the main OneNote interface. The main interface shows a note with the text "1134456732567" and "ເລີດບໍ່ຕ້ອງປະກາດນີ້".

A "Make a List..." dialog box is open in OneNote. A red arrow points from the "Apply Label" button in the previous screenshot to this dialog. The main interface shows a note with the text "ThaiCySex Footer ka" and "1134456732567".

User can apply label manually

One file, One label

Can add watermark in Word (not email)

A Microsoft Word document titled "SarahLabelTest" is shown. The ribbon has "AutoSave" selected. The status bar says "Changes are automatically saved to OneDrive. Last saved: 07:16.". The main content area shows a note with the text "Label for test in ThaiCySex ka 😊" and "ເຮືອບັນດາບໍ່ຕ້ອງປະກາດນີ້". A red callout box at the bottom right points to the text "Can add header/footer/watermarks to docs".



# SC-900

SECURITY  
COMPLIANCE  
IDENTITY



## Customer Lockbox

**Customer lockbox**

Provide additional security by requiring approvals through lockbox email requests for access to the data for your organization.

Microsoft 365

Action required

Require approval for all data access requests

**A Customer Lockbox request is pending your approval**

Sign in to the Microsoft 365 admin center to approve or deny this request.

**Request details**

Product	Exchange
Service Request #	0001-dc35d1f3-82ce-4378-82e4-a5c673784443
Request ID	0001-dc35d1f3-82ce-4378-82e4-a5c673784443
Tenant	Contoso
Requestor	Microsoft Operator
Reason	Troubleshoot issues impacting the customer's service
Create Time	8/28/2020 12:14:18 PM
Duration	12
Requestor's Location	United States
Expires	8/29/2020 12:14:18 PM

If a Customer Lockbox request is denied or isn't approved within 12 hours, the request expires. If this happens, you might continue to experience a specific service issue that could be resolved by allowing an engineer to access the content.

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

### Microsoft Engineer

Reference number	CLB#TEST02052018
Date requested (UTC)	2019-02-05 07:11:55 PM
Reason	Troubleshoot issues impacting the customer's service
Requestor	Microsoft Engineer
Duration	04:00:00
Action status	Pending
Service name	

### Microsoft Engineer

A Microsoft engineer has a 4-hour window with access to the content to troubleshoot this support issue. After this time, access is revoked regardless of whether the issue was resolved. You can track the status of this request from the Customer Lockbox Requests page. [Learn more about the process](#)

Close

# SC-900

SECURITY  
COMPLIANCE  
IDENTITY

The screenshot shows the Microsoft Purview interface with a 'Microsoft CERTIFIED' badge. The left sidebar includes 'Solutions' (Catalog, Audit, Content search, Communication compliance, Data loss prevention, eDiscovery), 'Audit', and 'Data loss prevention' (selected). A blue callout box says 'Can display policy tips'. The main area shows a 'Default policy for Teams' with 'Status: On' and a description: 'This policy detects the presence of credit card numbers in Teams chats and channel messages. When this sensitive information is detected, admins will get an Alert notification. Users would not see any policy tip. However, you can edit these actions anytime.' It also lists 'Locations to apply the policy' (Teams chat and channel messages) and 'Policy settings' (Default Teams DLP policy rule). A red callout box says 'Or protect docs contain sensitive info'.

## Data Loss Prevention (DLP)

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

The screenshot shows the 'compliance.microsoft.com/datalossprevention' portal. The top navigation bar includes 'InPrivate' and a user icon. The main page title is 'Data loss prevention > Create policy'. It says 'Start with a template or create a custom policy'. Below it, a list of steps is shown: 'Choose the information to protect' (selected), 'Name your policy', 'Locations to apply the policy', and 'Policy settings'. A callout box says 'Check out our new enhanced policy templates. These enhanced templates extend several of the original templates by also detecting named entities (such as full names and physical addresses). Just look for the templates labeled 'Enhanced' to start protecting even more personal data.' The 'Categories' section includes Enhanced, Financial, Medical and health, and Privacy. At the bottom are 'Next' and 'Cancel' buttons. A red THCS logo is in the bottom right corner.

## 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

Security policy violations (preview)

Health record misuse (preview)

### Categories

Data theft

Data leaks

### Categories

### 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 data leaks

Data leaks by priority users

Data leaks by disgruntled users (preview)

Many new template to find bad bad guys in your office

### General health record misuse (preview)

Detects health record misuse by a user included in this policy. Misuse can range from accessing privileged patient records to accessing records of patients from family or neighbors.



# SC-900

SECURITY  
COMPLIANCE  
IDENTITY



Can access directly  
from 365  
Compliance center  
(Purview)

The screenshot shows the Microsoft Purview Compliance Center interface. On the left, there's a navigation sidebar with a shield icon and the text "Microsoft CERTIFIED SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS". Below this, the "Insider risk management" section is highlighted. The main content area is titled "Insider risk management" and shows an "Overview" tab selected. It displays a list of top recommended actions:

Action	Type	Time
Turn on auditing	Required	2 min
Get permissions to use insider risk management.	Required	2 min
Choose policy indicators	Required	2 min
Scan for potential insider risks	Optional	48 hours
Assign permissions to others	Optional	5 min
Create your first policy	Required	5 min

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

[compliance.microsoft.com/insiderriskmgmt](https://compliance.microsoft.com/insiderriskmgmt)

## Choose a policy template

These templates are made up of conditions and indicators that define the risk activities you want to detect and investigate. All templates rely on a triggering event to occur before the policy will begin assigning risk scores to user activity. Triggering events are different depending on the template you choose, and prerequisites are required for some policies to work. [Learn more about templates](#)

To bypass triggering event requirements, you can temporarily assign risk scores to users based on activity detected in this policy. [Learn how to do this](#)

[Back to Templates](#)

### Data theft by departing users

Detects data theft by departing users near their resignation or termination date.

[Learn more about this template](#)

#### Prerequisites

- (Optional) HR data connector configured to periodically



Phishing is not  
“insider” risks

# SC-900

SECURITY  
COMPLIANCE  
IDENTITY



## (Basic) Audit

License: M365 E3

Audit user activities

Retain logs for 90 days

[compliance.microsoft.com/auditlogsearch](https://compliance.microsoft.com/auditlogsearch)

The screenshot shows the Microsoft Purview Audit log search interface. The left sidebar lists various compliance categories like Security, Data Catalog, Audit, and more. The main area has a title "Audit" with tabs for "Search" (selected), "New Search (Preview)", and "Audit retention policies". It includes filters for "Date and time range" (from Feb 1, 2022, to Jan 6, 2022), "Activities" (Copied file), and "File, folder, or site" (Enter all or a part of). Below these are sections for "Users" and "Add the users whose audit logs". A note at the bottom states: "Search results might be impacted by audit log retention policies. Activities that happened over 90 days ago will only show up in results for users who have licensing for long-term audit log retention." At the bottom are "Search" and "Clear all" buttons. To the right, a detailed table of audit logs is shown for the period from Thursday, Jan 6, 2022, 17:00:00 to Thursday, Jul 21, 2022, 17:00:00. The table has columns: Date, IP Address, User, Activity, Item, and Detail. The results show four items, all of which were deleted files.

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



# SC-900

SECURITY  
COMPLIANCE  
IDENTITY



SECURITY,  
AND  
FUNDAMENTALS

## Audit

Purview Audit (Premium) (E5)

## Advance Audit

Retain up to 10 years

More events: MailItemsAccessed

Customer-dedicate bandwidth

compliance.microsoft.com/auditlogsearch

The screenshot shows the Audit interface with the following details:

- Date and time range \***: Start: Wed, 00:00; End: Sat, 00:30.
- Activities**: Accessed mailbox items. A dropdown menu lists other options like "Copied messages to an..." and "User signed in to mailbox".
- File, folder, or site ⓘ**: Enter all or a part of the na... (partially visible).
- Search name**: ThaiCySec Advance Audit.
- Buttons**: Search, Clear all.
- Bottom navigation**: Copy this search, Delete, Refresh, Progress(%), Search Ti..., Number of results, Creation time ↓, Searched by...

A red arrow points from the "Accessed mailbox items" filter to the text "Can identity when users use search bar in Outlook".

The screenshot shows the Audit retention policies interface with the following details:

- Audit retention policies** section: Policy name \*: ThaiCySec Retent 10yrs, Description: เก็บได้ถึง 10 ปีเชียว.
- Users**: Search, Record type: Yammer, Exchangeitem.
- Duration \***: 90 Days, 6 Months, 9 Months, 1 Year, 10 Years (selected).
- Priority \***: 10.
- Buttons**: Save, Cancel.

A red arrow points from the "Audit retention policies" section to the text "Cannot view content of email message".

The bottom part shows a search results page with the URL "compliance.microsoft.com/auditlogsearch". It displays a table with one row:

New Search (Preview)	Search	Audit retention policies
ThaiCySec Retent 10yrs	Priority: 10	Record type: Yammer, Exchangeitem

A red arrow points from the table to the text "Nothing about billing details (audit data, not 365 bill)".



## Content Search

Identify docs in Email/Sharepoint contain keywords

The screenshot shows the Microsoft Purview Content Search interface. On the left, a sidebar titled 'New search' has 'Locations' selected. Below it, 'Define your search conditions' includes a 'Keywords' input field containing 'thaicysec'. A 'Next' button is at the bottom.

The screenshot shows the Microsoft Purview Content search results page. It displays a list of search samples with columns for Subject/Title, Date, and Sender/Author. The results include:

Subject/Title	Date	Sender/Author
No Subject	May 17, 2022 7:16 PM	No Sender
Verify your email address with TikTok	Jan 6, 2022 1:12 PM	noreply@account.tiktok.com
No Subject	May 17, 2022 7:16 PM	No Sender
You've joined the ThaiCySec 2022 Events group	May 17, 2022 7:20 PM	ThaiCySec2022Events@nol121.onmicrosoft.com
No Subject	May 17, 2022 7:16 PM	No Sender

# SC-900

SECURITY  
COMPLIANCE  
IDENTITY



## Content Search

Can see full content  
or even download  
them

Identify docs in Email/Sharepoint  
contain keywords

The screenshot shows a Microsoft Edge browser window with the URL <https://compliance.microsoft.com/contentsearchv2?viewid=search>. The page title is "ThaiCySec content search samples". The search bar contains the text "ake ake". The results table has columns for "Subject/Title", "Date", and "Sender/Author". There are ten items listed:

Subject/Title	Date	Sender/Author
No Subject	May 17, 2022 7:16 ...	No Sender
Verify your email address...	Jan 6, 2022 1:12 PM	noreply@account.tiktok...
No Subject	May 17, 2022 7:16 ...	No Sender
You've joined the ThaiCy...	May 17, 2022 7:20 ...	ThaiCySec2022Eve...
No Subject	May 17, 2022 7:16 ...	No Sender
The new ThaiCySec 2022...	May 17, 2022 7:05 ...	ThaiCySec2022Eve...
You've joined the ThaiCy...	May 17, 2022 7:20 ...	ThaiCySec2022Eve...
You've joined the ThaiCy...	May 17, 2022 7:20 ...	ThaiCySec2022Eve...
No Subject	May 17, 2022 7:16 ...	No Sender

Below the table is a "Load more items" button. To the right of the table, there is a "Subject line" section with a "Download Original Item" link. Further down, there is a "Source" section showing the details of the selected email from TikTok, including the "From" field (TikTok <noreply@account.tiktok.com>), "To" field (redacted), "Subject" field (Verify your email address with TikTok), and "Send Date" (1/6/2022 6:11:52 AM (UTC)). Below this is a "Download Original Item" link. At the bottom of the page, there is a "TikTok" logo and the text "Hi ThaiCySec". The footer of the page says "Thanks for joining TikTok! TikTok is not only a destination for".



# SC-900

SECURITY  
COMPLIANCE  
IDENTITY



Microsoft Azure Search resources, services, and docs (G+/-) DEFAULT DIRECTORY

Home > Policy

Overall resource compliance 0% 0 out of 5

Resources by compliance state: 5 (0 - Compliant, 0 - Exempt, 5 - Non-compliant)

Non-compliant initiatives 2 0 out of 2

Non-compliant policies 76 0 out of 391

Name	Scope	Compliance state	Resource compli...	Non-Compliant ...	Non-compli...
ASC Default (subscr...	Visual Studio Enterpr...	✗ Non-compliant	0% (0 out of 4)	4	51
Configure Azure Ac...	Visual Studio Enterpr...	✗ Non-compliant	0% (0 out of 1)	1	1
ASC Default (subscr...	Pay-As-You-Go	✗ Non-compliant	0% (0 out of 1)	1	24

## Azure Policy

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

... > Policy > Configure Azure Activity logs to stream to specified Log Analytics workspace

### Configure Azure Activity logs to stream to specific

Edit Policy Assignment

Basics Parameters Remediation Non-compliance messages Review + save

By default, this assignment will only take effect on newly created resources. Existing resources can be updated via a remediation task after the policy is assigned. For deployIfNotExists policies, the remediation task will deploy the specified template. For modify policies, the remediation task will edit tags on the existing resources.

Create a remediation task

Policy to remediate

Configure Azure Activity logs to stream to specified Log Analytics workspace



# SC-900

SECURITY  
COMPLIANCE  
IDENTITY



## Azure Blueprint

Provision resources across subscriptions in consistent manner

The screenshot illustrates the process of creating and assigning an Azure Blueprint.

**Create blueprint:** The user is in the "Artifacts" tab, adding artifacts such as "Subscription", "VNET Resource Group", "NSG for new VNET", and "VNET and one subnet".

**Assign blueprint:** The user is assigning the blueprint "ThaiCySec-TestBlueprint" to the "Visual Studio Enterprise Subscription" in the "West US 2" location. The blueprint definition version is set to 1.0. The "Lock Assignment" section shows options for "Don't Lock", "Do Not Delete", and "Read Only". The "Managed Identity" scope is set to "System assigned".

**Blueprint definitions:** The user is viewing the "Blueprint definitions" page, which lists the assigned blueprint "ThaiCySec-TestBlu...".

**Assigned blueprints:** A context menu for the assigned blueprint shows options: "View blueprint", "Publish blueprint", "Edit blueprint", and "Delete blueprint".

**Artifact parameters:** The "Subscription" artifact parameter is set to "[concat(parameters('resou...")]. The "VNET Resource Group" artifact parameter includes fields for "Resource Group: Name" and "Resource Group: Location". The "NSG for new VNET" artifact parameter includes fields for "Address space for vnet" and "Address space for subnet". The "VNET and one subnet" artifact parameter includes fields for "Address space for vnet" and "Address space for subnet".





Microsoft Azure

Search resources, services, and docs (G+/)

Home > ThaiCySecTestVM\_group

## ThaiCySecTestVM\_group | Locks

Resource group

Search (Ctrl+ /)

Add Subscription Refresh Feedback

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Deployments

Security

Policies

Properties

Locks

### Add lock

Lock name \*

ThaiCySecLock11

Lock type \*

Read-only

Notes

Read-only

Delete

OK

Cancel

Scope

ThaiCySecTestVM\_group

ThaiCySecTestVM\_group

ThaiCySecTestVM\_group

ThaiCySecTestVM\_group

ThaiCySecTestVM\_group

ThaiCySecTestVM\_group

ThaiCySecTestVM\_group

ThaiCySecTestVM\_group

ThaiCySecTestVM\_group

## 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



## Exam Example in SC-900



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.

About Sensitivity Label:

1. Can add custom watermark to Word documents?
2. Can add custom watermark to Email?
3. Can add custom header/footer to documents?
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



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



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



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 (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



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



### About Insider Risk:

1. You can manage Insider Risk from M365 (Purview) Compliance portal
2. You can access Insider Risk management at security.microsoft.com portal
3. Phishing is one Insider Risk you can manage
4. Data Breach from unhappy employee is one Insider Risk you can manage

Yes/No
Yes/No
Yes/No
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



### About Compliance Manager:

1. Have many predefined Compliance template to use
2. Can check how much you comply with variety of standards
3. Can check compliance with Thailand PDPA
4. Cannot track controls that Microsoft-side manage

Yes/No
Yes/No
Yes/No
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.

## 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.