

NAME: KSHITIJ GUPTA
Enrolment Number: 21162101007
Sub: CS

Practical – 1[Batch-71]

Your organization, XYZ Corp, is migrating its e-commerce platform to the IBM Cloud. As a part of this migration, the company needs to ensure that the new cloud environment complies with industry regulations such as PCI-DSS for handling payment information and GDPR for protecting customer data. The goal is to implement IBM Cloud Security and Compliance Center to continuously monitor and maintain the security and compliance posture of the e-commerce platform.

Go through the requirements and perform the following tasks:

1: Provision the Security and Compliance Center:

- Log in to XYZ Corp's IBM Cloud account.
- Navigate to the Security and Compliance Center and provision the service.

2: Configure the Service:

- Connect the e-commerce platform's cloud resources to the Security and Compliance Center.
- Enable data collection for security and compliance metrics.

3: Define and Apply Policies:

- Identify PCI-DSS and GDPR compliance requirements.
- Create and apply security and compliance policies within the Security and Compliance Center.

4: Run Initial Security Scans:

- Initiate security scans on the e-commerce platform.
- Analyze results to identify and prioritize issues.

5: Remediate Identified Issues:

- Develop and implement remediation plans.
- Validate changes to ensure issues are resolved effectively.

6: Enable Continuous Monitoring, Review and Improve:

- Set up continuous monitoring and configure alerts.
- Generate and review compliance reports regularly.
- Conduct regular reviews and update policies and procedures.

Search for Security and Compliance Center (Service) and select location and create service.

The screenshot shows a browser window for the IBM Cloud Catalog. The URL is cloud.ibm.com/catalog/services/security-and-compliance-center. The page displays the 'Security and Compliance Center' service details. On the left, there's a sidebar with service filters like Type (Service), Provider (IBM), and Location (Dallas). The main content area shows the service name, location (Dallas), and a summary table with plan details. A 'Create' button is visible at the bottom right of the main content area. The status bar at the bottom shows system information including weather (26°C Rain), battery level (15:03), and date (27-08-2024).

Plan	Features and capabilities	Pricing
Trial	Try Security and Compliance Center at no cost for 30 days	Free
Standard	Pay per evaluation	₹1,120,224.14 INR/Evaluation

Screenshot of the IBM Cloud Security and Compliance Center trial page.

Category: Security

Compliance: Financial Services, Validated, IAM-enabled, Service Endpoint Supported

Location: Toronto, Frankfurt, Madrid, Dallas

Related links: Docs, Terms

Configure your resource:

- Service name: Security and Compliance Center-KGupta
- Select a resource group: default
- Tags: Examples: env:dev, version-1

Summary:

Security and Compliance Center Free

Location: Dallas
Plan: Trial
Service name: Security and Compliance Center-KGupta
Resource group: default

I have read and agree to the following license agreements: [Terms](#)

Create, Add to estimate

Screenshot of the IBM Cloud Security and Compliance Center overview page.

Instances: Security and Compliance ...

Overview: Get started → Create instance +

Manage the security and compliance of your workloads

Define, implement, and assess the security and compliance controls that are required for your organization.

Use case: Financial services

- 01 Define your requirements
- 02 Implement secure deployments
- 03 Assess your posture

Go to Controls then Control Libraries and select for the following library.

The screenshot shows the IBM Cloud interface for Security and Compliance. The left sidebar is titled 'IBM Cloud' and includes sections for 'Security and Compliance', 'Instances', 'Overview', 'Monitor', 'Dashboard', 'Manage', 'Controls', 'Control libraries' (which is currently selected), 'Rules', 'Profiles', 'Attachments', 'Integrations', and 'Plan'. The main content area is titled 'Control libraries' and displays a table of available controls. A yellow warning box at the top right says 'Plan' followed by 'Your Trial plan expires in 29 days. To ensure that your scans are not interrupted, upgrade to the Standard plan.' with a 'Upgrade' button. The table has columns for 'Name', 'Type', 'Controls', and 'Last modified'. The first four rows are Predefined benchmarks from CIS and AWS, and the fifth row is a 'CIS IBM Cloud Foundations Benchmark v1.1.0 (1.1.0)'. A search bar at the top of the table area contains 'foundation'. The bottom status bar shows the URL 'https://cloud.ibm.com/security-compliance/crn%3Av1%3Abuemix%3Apublic%3Acompliance%3Aus-south%3Aa%2F9553f5f7184ddb922a056f240cf78ef6%3A440711d4-9a9f-4f7a-bfe9-a1a9a622...', the date '27-08-2024', and the time '15:09'.

Here we can see all the controls available.

The screenshot shows the 'Details' page for the CIS IBM Cloud Foundations Benchmark version 1.0. It includes sections for 'Choose a version to review' (set to 1.1.0), 'Description' (CIS IBM Cloud Foundations Benchmark version 1.0), 'ID' (51ca566e-c559-412b-8d64-f05b57044c32), 'Updated on' (08/27/2024, 7:43 AM), 'Created by' (IBM Cloud), 'Type' (Predefined), and 'Controls' (67). Below this is a table grouped by control, showing 1.1.0 through 1.1.6. The bottom status bar shows the URL 'https://cloud.ibm.com/security-compliance/crn%3Av1%3Abuemix%3Apublic%3Acompliance%3Aus-south%3Aa%2F9553f5f7184ddb922a056f240cf78ef6%3A440711d4-9a9f-4f7a-bfe9-a1a9a622...', the date '27-08-2024', and the time '15:10'.

Now go to Attachments.

Security and Compliance

Instances

Security and Compliance ...

Overview

Monitor

Dashboard

Manage

Controls

Profiles

Attachments

Integrations

Plan

Settings

Attachments

An attachment is the connection between a profile and a set of resources that defines the way an evaluation is conducted.

Plan

Your Trial plan expires in 29 days. To ensure that your scans are not interrupted, upgrade to the Standard plan.

Upgrade

Create

Now we will create an attachment and enter all the details.

Security and Compliance / Attachments / Create an attachment

Details

Name

Testing-007

Description (optional)

Testing _PR1

Cancel

Back

Next

Security and Compliance - IBM

cloud.ibm.com/security-compliance/crn%3Av1%3Abuemix%3Apublic%3Acompliance%3Aus-south%3Aa%2F9553f5f7184ddb922a056f240cf78ef6%3A440711d4-9a9f-4f7a-bfe9-a1a9a622...

Inbox (1) - kshitijgu... Apps WhatsApp Home / Twitter Electronic library, D... Subtraction of two... Instagram TITLE.PMS Swift Home - Chess.com LinkedIn Login, Sign... All Bookmarks

IBM Cloud Search resources and products... Catalog Manage 2716063 - IBM India Pvt Ltd, C...

Create an attachment

Details Profile Scope Scan settings Review

Profile Select a profile

Storage To allow Sec Cloud Object Connect

Profile AI ICT Guard Cancel

Service authorization required To allow Security and Compliance Center to communicate with Cloud Object Storage, create an authorization. The required permissions are pre-selected on the next screen.

Learn more. Authorize

Type here to search 26°C Rain 15:13 27-08-2024

Security and Compliance - IBM

cloud.ibm.com/security-compliance/crn%3Av1%3Abuemix%3Apublic%3Acompliance%3Aus-south%3Aa%2F9553f5f7184ddb922a056f240cf78ef6%3A440711d4-9a9f-4f7a-bfe9-a1a9a622...

Inbox (1) - kshitijgu... Apps WhatsApp Home / Twitter Electronic library, D... Subtraction of two... Instagram TITLE.PMS Swift Home - Chess.com LinkedIn Login, Sign... All Bookmarks

IBM Cloud Search resources and products... Catalog Manage 2716063 - IBM India Pvt Ltd, C...

Create an attachment

Details Profile Scope Scan settings Review

Profile Select a profile

Storage To allow Sec Cloud Object Connect

Profile AI ICT Guard Cancel

Authorize service to service access for Security and Compliance

Select a target service Select a target service for Security and Compliance to access as the source service. Only one service can be added at a time.

Target service Cloud Object Storage

region Region All regions

serviceInstance string equals serviceInstance

resource string equals

resourceType

Type here to search 26°C Rain 15:14 27-08-2024

Security and Compliance / Attachments / Create an attachment

Profile

Select a profile

Cloud Object Storage

Region: All regions

serviceInstance: string equals Cloud Object Storage-007 (45d63717-9c)

resource: string equals

resourceType: string equals

Access

Select a target service for Security and Compliance to access as the source service. Only one service can be added at a time.

Target service: Cloud Object Storage

region: Region: All regions

serviceInstance: string equals Cloud Object Storage-007 (45d63717-9c)

resource: string equals

resourceType: string equals

Review

Security and Compliance / Attachments / Create an attachment

Profile

Select a profile

Cloud Object Storage

Region: All regions

serviceInstance: string equals Cloud Object Storage-007 (45d63717-9c)

resource: string equals

resourceType: string equals

Access

Select a role to determine the level of access for the source service.

Service access: Writer As a Writer, one can create/modify/delete buckets. In addition, one can upload and download the objects in the bucket.

Review

Screenshot of the IBM Cloud Security and Compliance interface showing the 'Create an attachment' process.

The main window shows a sidebar with steps: Details, Profile, Scope, Scan settings, and Review. The Profile step is active, displaying a 'Profile' section with a 'Cloud Object Storage' instance selected. A modal dialog titled 'Review service to service authorization for Security and Compliance' is open, asking for review assignment before creating access. It shows the target service as 'Cloud Object Storage' and a role of 'Writer'. The 'Assign' button is highlighted in blue.

Screenshot of the IBM Cloud Security and Compliance interface showing the 'Create an attachment' process.

The main window shows a sidebar with steps: Details, Profile, Scope, Scan settings, and Review. The Profile step is active, displaying a 'Profile' section with a 'Cloud Object Storage' instance selected. A modal dialog titled 'Connect storage' is open, prompting to connect a Cloud Object Storage bucket. It shows a dropdown for 'Cloud Object Storage instance' set to 'Cloud Object Storage-007' and a table for 'Cloud Object Storage buckets' containing one entry: 'ktesting' with 'smart' storage class and 'us' location. The 'Connect' button is highlighted in blue.

Security and Compliance / Attachments / Create an attachment

Scope

Target a scope to define the way that your evaluation is conducted.

Scope ⓘ

Ganpat-2021-Sem6-rg

Select exclusions

Select a target account scope(s)

Cancel Back Next

Select any bucket testsecurityandcompliance and connect.

Security and Compliance / Attachments / Create an attachment

Profile

Select a profile to define the way that your evaluation is conducted.

Profile ⓘ

AI ICT Guardrails (1.0.0)

Parameters

Description	Parameters	Component
Check whether Toolchain is configured only with the allowed integration tools	1	Toolchain
Check whether Container Registry Vulnerability Advisor scans for critical or high vulnerabilities in the system at least every # day(s)	1	Container Registry

Cancel Back Next

Security and Compliance - IBM Cloud Object Storage - IBM Cloud Object Storage - IBM Cloud

Inbox (1) - kshitijgu... Apps WhatsApp Home / Twitter Electronic library, D... Subtraction of two... Instagram TITLE.PMS Swift Home - Chess.com LinkedIn Login, Sign... All Bookmarks

IBM Cloud Search resources and products... Catalog Manage 2716063 - IBM India Pvt Ltd, C...

Security and Compliance / Attachments Create an attachment

Details Profile Scope Scan settings Review

Scope Target a scope to define the way that your evaluation is conducted.

Scope Ganpat-2021-Sem6-rg

Exclude resource groups (optional)

Select exclusions

Target account scope (optional)

Select a target account scope(s)

Cancel Back Next

Type here to search 26°C Rain ENG 15:30 27-08-2024

Security and Compliance - IBM Cloud Object Storage - IBM Cloud Object Storage - IBM Cloud

Inbox (1) - kshitijgu... WhatsApp Home / Twitter Electronic library, D... Subtraction of two... Instagram TITLE.PMS Swift Home - Chess.com LinkedIn Login, Sign... All Bookmarks

IBM Cloud Search resources and products... Catalog Manage 2716063 - IBM India Pvt Ltd, C...

Security and Compliance Instances Security and Compliance ...

Overview Monitor Dashboard

Manage Controls Profiles Attachments Integrations Plan Settings

Attachments An attachment is the connection between a profile and a set of resources that defines the way an evaluation is conducted.

Plan Your Trial plan expires in 29 days. To ensure that your scans are not interrupted, upgrade to the Standard plan. Upgrade

Name	Profile	Environment	Last scanned	Next scan	Status	Updates
KSHITIJ GUPTA	AI ICT Guardrails (1.0.0)	IBM Cloud	08/27/2024, 4:11 PM	Scan in progress	Latest version	-

Type here to search 26°C Rain ENG 16:12 27-08-2024

The screenshot shows the IBM Cloud Security and Compliance interface. The left sidebar is titled "IBM Cloud" and includes sections for Security and Compliance, Overview, Monitor, Dashboard, Manage, Controls, Profiles, Attachments (which is currently selected), Integrations, Plan, and Settings. The main content area is titled "Attachments" and contains a sub-header: "An attachment is the connection between a profile and a set of resources that defines the way an evaluation is conducted." Below this is a yellow warning box titled "Plan" with the message: "Your Trial plan expires in 29 days. To ensure that your scans are not interrupted, upgrade to the Standard plan." A "Upgrade" button is located in the top right corner of this box. To the right of the warning box is a table with columns: Name, Profile, Environment, Last scanned, Next scan, Status, and Updates. One row is visible, showing "KSHITIJ GUPTA" as the Name, "AI ICT Guardrails (1.0.0)" as the Profile, "IBM Cloud" as the Environment, "08/27/2024, 4:11 PM" as the Last scanned date, "08/28/2024" as the Next scan date, "Latest version" as the Status, and a minus sign as the Updates indicator. At the bottom right of the main content area is a "Create" button with a plus sign. The Windows taskbar at the bottom shows various pinned icons and the system tray.

Click on the attachment and click the profile details

This screenshot shows the same IBM Cloud interface as the previous one, but the "Attachment details" for the profile "KSHITIJ GUPTA" are displayed in a modal window. The modal has a "Close" button in the top right corner. The left side of the modal shows the "Attachments" list, which is identical to the one in the main window. The right side displays the "Attachment details" for the selected profile. It includes fields for Name (KSHITIJ GUPTA), Description (optional testing), ID (bb6c8f3c-d8da-48b5-9ac3-94139a629dac), Profile name (AI ICT Guardrails (1.0.0)), and a "Scope" tab. The "Scope" tab shows the environment "IBM Cloud" and the scope "Ganpat-2021-Sem6-rg". Other tabs include "Scan settings" and "Parameters". The Windows taskbar at the bottom is visible.

Screenshot of the IBM Cloud Security and Compliance service showing the "AI ICT Guardrails" profile details.

Plan: Your Trial plan expires in 29 days. To ensure that your scans are not interrupted, upgrade to the Standard plan. [Upgrade](#)

Overview [Attachments \(1\)](#)

Version details

Choose a version to review 1.0.0	Controls 17	Published 12/10/2023, 11:46 PM	Status Latest version
Environment IBM Cloud	Type Predefined	ID 8a752a78-1e02-40e0-a60a-c245b16e018d	View

Description
The AI ICT guardrails provides a predefined list of infrastructure and data controls, required to handle AI and Generative AI(GenAI) workloads. These controls include AI specific elaborations across control categories like Risk and Compliance Management, Unified Infrastructure Security and Performance, Application and Workload Protection, Data Protection, Identity and Access Management, Logging, Monitoring. This list of controls is to be used in conjunction with the security baseline of the organization.

Grouped by control | Grouped by specification | Grouped by component | Grouped by category

Category: All | Assessments: Has Assess... | Search | Type here to search | 26°C Rain | 1632 | ENG | 27-08-2024

In dashboard on service home, the results are mentioned

Screenshot of the IBM Cloud Security and Compliance service showing the "Dashboard" view.

Instances: Security and Compliance ...

Overview

Monitor

Dashboard (selected)

Manage

Controls

Profiles

Attachments

Integrations

Plan

Settings

Dashboard

Plan: Your Trial plan expires in 29 days. To ensure that your scans are not interrupted, upgrade to the Standard plan. [Upgrade](#)

Success rate: 82%
345 / 416 evaluations passed

Total controls: 17 Controls

Compliant	Non-compliant	Unable to Perform
2	7	6

Total evaluations: 416 Evaluations

Passed	Failed	Unable to Perform
70	1	345

Click on the attachment to check its detailed results

Screenshot of the IBM Cloud Security and Compliance dashboard for user KSHITIJ GUPTA. The dashboard shows an evaluation pass rate of 82% with 416 total evaluations. It includes sections for Controls, Resources, and Drift, along with a detailed breakdown of evaluated controls.

Evaluation pass rate: 82%

Total evaluations	416
Passed evaluations	345
Resources evaluated	219
Controls evaluated	17

Controls:

Resources:

Drift:

7 days (selected) | 14 days | 30 days | 60 days | 90 days | 180 days | 365 days

In controls, it shows the security problems like here in case of object storage public access and managed keys

Screenshot of the IBM Cloud Security and Compliance dashboard for user KSHITIJ GUPTA. The dashboard shows an evaluation pass rate of 82% with 416 total evaluations. It includes sections for Controls, Resources, and Drift, along with a detailed breakdown of evaluated controls.

Controls:

Name	Description	Category	Specifications	Evaluation
ADP 1.1	Deploy mechanism for unified data governance, traceability and data residency across ICT infrastructure 1. Ensure unified data governance across hybrid multicloud ICT - on premises, cloud, and edge infrastructure environments 2. Ensure data meets local/regional residency requirements	Advanced Data Protection	2	
ADP 1.2	Implement safeguards for input data restrictions - * preventing input manipulation and malicious prompt injection * not divulging personal/sensitive/confidential information and protecting intellectual property. 1. Implement data discovery, classification and labelling 2. Protect Cloud Storage instances, providing data encryption for at-rest and in-motion data 3. Protect sensitive data, intellectual property data in use, leveraging advanced data protection technologies like homomorphic encryption	Advanced Data Protection	21	
ADP 1.3	Deploy mechanisms to protect output data, including metadata, from unauthorized access 1. Output data should not divulge sensitive or confidential information 2. Encrypt sensitive/confidential/intellectual property data at rest, in transit and data in use 3. Enable data protection for backup data	Advanced Data Protection	21	
AES 1.1	Define and deploy secure development practices for applications handling AI workloads. 1. Educate developers on security threats to AI workloads and train on secure coding practices	Application and Workload Protection	13	
AES 1.2	Deploy testing measures, including red teaming for adversarial testing, throughout the application development and workload handling 1. Perform testing in secure environments and at several checkpoints throughout the AI workload lifecycle in particular before deployment	Application and Workload Protection	3	

In dashboard of security service, click on the details of control and check the recommended remediation to solve the issue

The screenshot shows the IBM Cloud Security and Compliance interface. On the left, there's a sidebar with various compliance controls listed under sections like ADP 1.3, AES 1.1, AES 1.2, AES 1.3, and AES 1.4. The main content area displays a "Control specification details" section with a "Description" field containing the text "Ensure Event Streams is enabled with customer-managed encryption and Keep Your Own Key (KYOK)". Below this, there's a table with columns for Type (Automated), Method (IBM Cloud rule), Component (Event Streams), and Status (Compliant). Under the "Assessments" section, there's a single entry titled "Check whether Event Streams is enabled with customer-managed encryption and Keep Your Own Key (KYOK)" with an "Automated" status. The bottom of the screen shows a Windows taskbar with various pinned icons and system status.

Also the scan can be run at custom time by option visible in attachments tab on service home

The screenshot shows the IBM Cloud Security and Compliance interface with the "Attachments" tab selected in the sidebar. The main content area displays a table of attachments. There is one row visible for "KSHITIJ GUPTA" with the profile "AI ICT Guardrails (1.0.0)", environment "IBM Cloud", last scanned date "08/27/2024, 4:11 PM", next scan date "08/28/2024", status "Latest version", and updates count "-". A context menu is open over this row, showing options: "Edit", "Run scan", "View scan results", "Pause scan", and "Delete". The bottom of the screen shows a Windows taskbar with various pinned icons and system status.

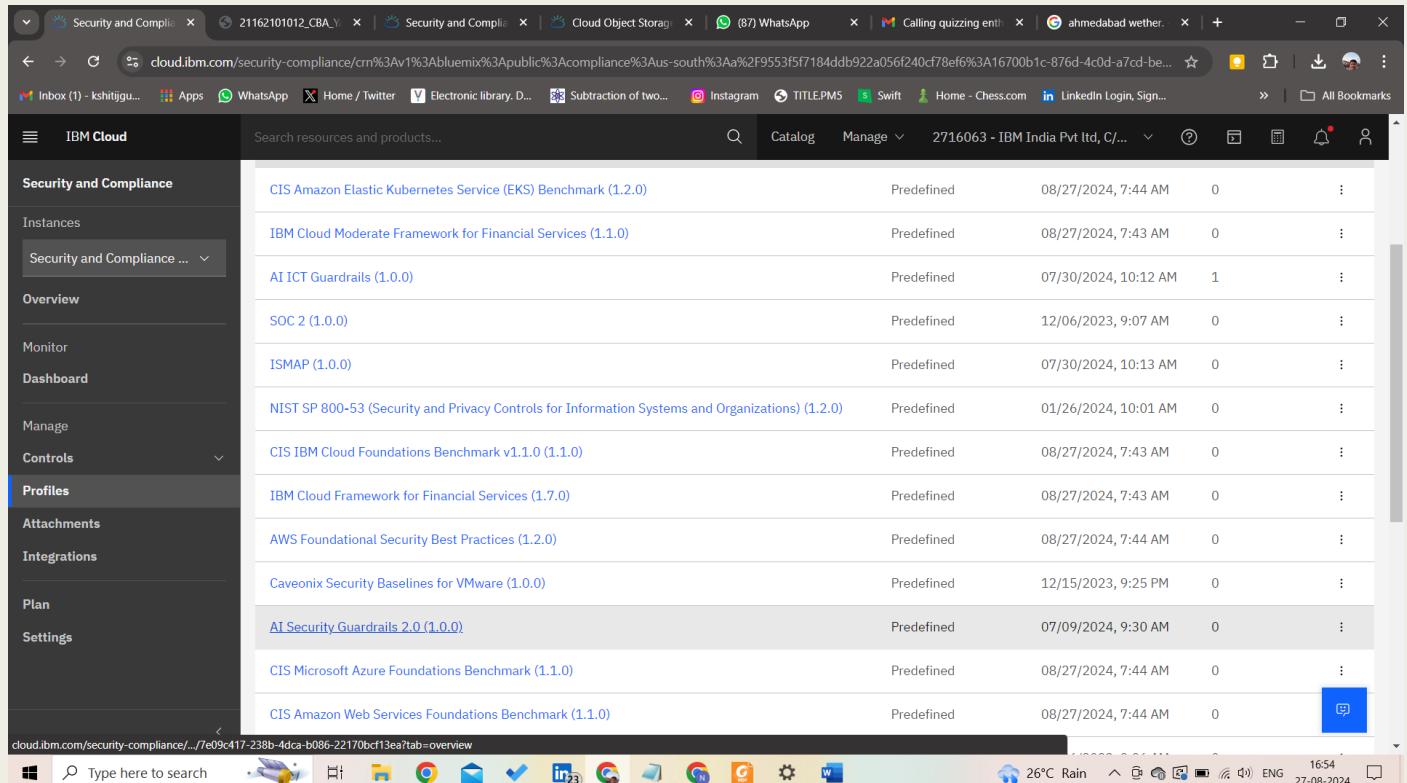
The screenshot shows the IBM Cloud Security and Compliance interface. The left sidebar is titled 'Security and Compliance' and includes sections for Instances, Overview, Monitor, Dashboard, Manage, Controls, Profiles, Attachments (which is selected), Integrations, Plan, and Settings. The main content area is titled 'Attachments' and contains a sub-header: 'An attachment is the connection between a profile and a set of resources that defines the way an evaluation is conducted.' A yellow warning box at the top says 'Plan' followed by 'Your Trial plan expires in 29 days. To ensure that your scans are not interrupted, upgrade to the Standard plan.' Below this is a table with columns: Name, Profile, Environment, Last scanned, Next scan, Status, and Updates. One row is shown: 'KSHITIJ GUPTA' (Profile: AI ICT Guardrails (1.0.0)), Environment: IBM Cloud, Last scanned: 08/27/2024, 4:39 PM, Next scan: 08/28/2024, Status: Latest version, Updates: -. At the bottom of the table is a 'Create' button. The browser taskbar at the bottom shows various open tabs and system icons.

The screenshot shows the same IBM Cloud Security and Compliance interface as the previous one, but the modal window from the first screenshot is no longer present. The yellow warning box at the top still displays the trial expiration notice. The table below remains the same, showing the single attachment entry for 'KSHITIJ GUPTA'. The browser taskbar at the bottom is identical to the first screenshot.

TASK : Identify AI Security Guardrails 2.0 (1.0.0) compliance requirements. Create an Attachment using the predefined AI Security Guardrails profile and initiate security scans. Analyze results to identify issues and Validate any 3 changes to ensure issues are resolved effectively. Example: Toolchain issues, key protect

issues, IBM cloud object storage issues, and Watson Machine learning issues can be rectified.

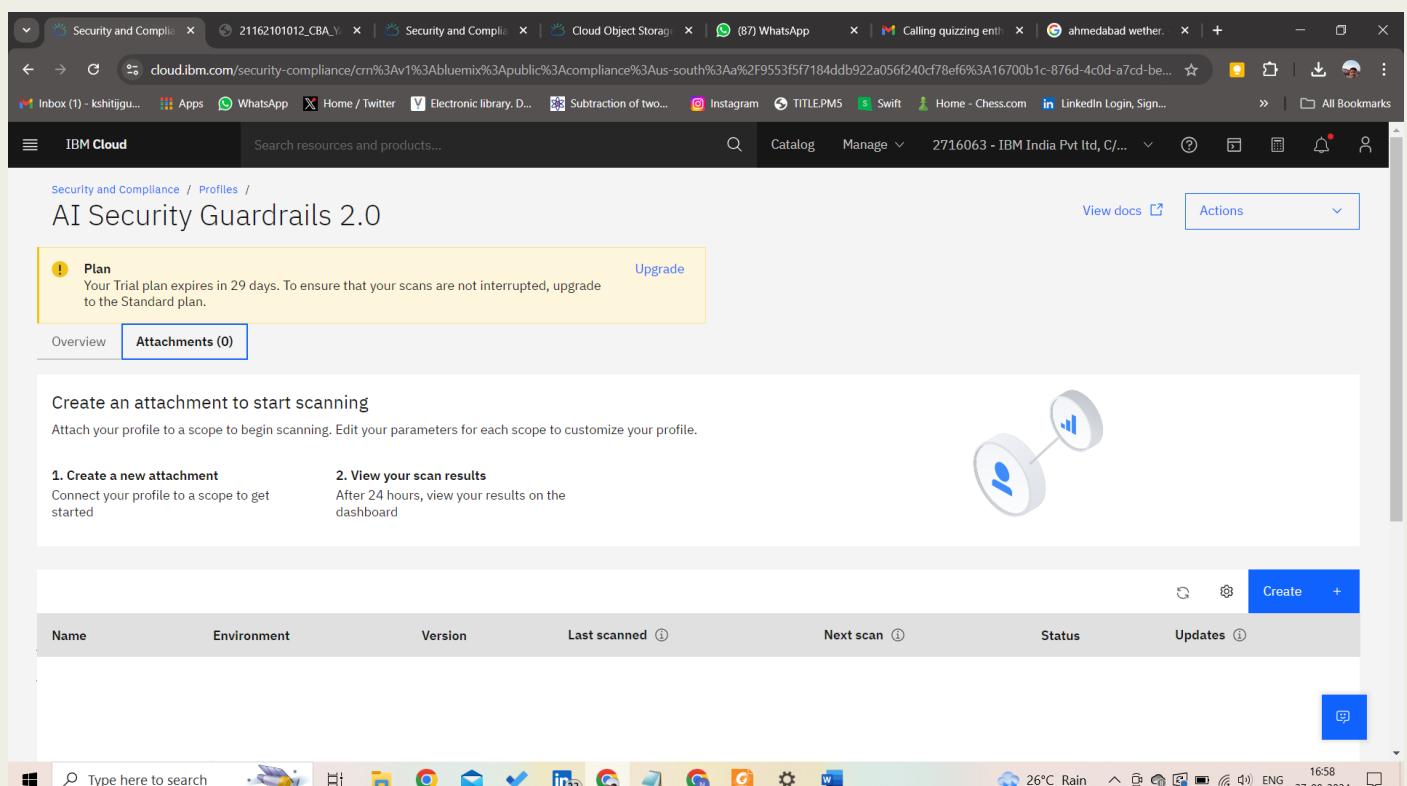
Visit AI Security Guardrails profile



The screenshot shows the IBM Cloud Security and Compliance Profiles page. The left sidebar is titled "IBM Cloud" and includes sections for "Security and Compliance", "Instances", "Overview", "Monitor", "Dashboard", "Manage", "Controls", "Profiles" (which is selected), "Attachments", "Integrations", "Plan", and "Settings". The main content area displays a list of predefined profiles:

Profile Name	Type	Last Updated	Scans	Actions
CIS Amazon Elastic Kubernetes Service (EKS) Benchmark (1.2.0)	Predefined	08/27/2024, 7:44 AM	0	⋮
IBM Cloud Moderate Framework for Financial Services (1.1.0)	Predefined	08/27/2024, 7:43 AM	0	⋮
AI ICT Guardrails (1.0.0)	Predefined	07/30/2024, 10:12 AM	1	⋮
SOC 2 (1.0.0)	Predefined	12/06/2023, 9:07 AM	0	⋮
ISMAP (1.0.0)	Predefined	07/30/2024, 10:13 AM	0	⋮
NIST SP 800-53 (Security and Privacy Controls for Information Systems and Organizations) (1.2.0)	Predefined	01/26/2024, 10:01 AM	0	⋮
CIS IBM Cloud Foundations Benchmark v1.1.0 (1.1.0)	Predefined	08/27/2024, 7:43 AM	0	⋮
IBM Cloud Framework for Financial Services (1.7.0)	Predefined	08/27/2024, 7:43 AM	0	⋮
AWS Foundational Security Best Practices (1.2.0)	Predefined	08/27/2024, 7:44 AM	0	⋮
Caveonix Security Baselines for VMware (1.0.0)	Predefined	12/15/2023, 9:25 PM	0	⋮
AI Security Guardrails 2.0 (1.0.0)	Predefined	07/09/2024, 9:30 AM	0	⋮
CIS Microsoft Azure Foundations Benchmark (1.1.0)	Predefined	08/27/2024, 7:44 AM	0	⋮
CIS Amazon Web Services Foundations Benchmark (1.1.0)	Predefined	08/27/2024, 7:44 AM	0	⋮

Create new attachment



The screenshot shows the "AI Security Guardrails 2.0" attachments creation page. The top navigation bar includes links for "Security and Compliance / Profiles / AI Security Guardrails 2.0", "View docs", and "Actions". The main content area has a "Plan" section with a warning about a trial plan expiring in 29 days and a link to "Upgrade". Below this are two tabs: "Overview" (selected) and "Attachments (0)". A large callout box says "Create an attachment to start scanning" and "Attach your profile to a scope to begin scanning. Edit your parameters for each scope to customize your profile." It lists two steps: "1. Create a new attachment" (Connect your profile to a scope to get started) and "2. View your scan results" (After 24 hours, view your results on the dashboard). To the right is a "Create" button and a "Scan" icon. At the bottom is a table with columns: Name, Environment, Version, Last scanned, Next scan, Status, and Updates. The table is currently empty.

Screenshot of the IBM Cloud Security and Compliance interface showing the 'Create an attachment' step.

The left sidebar shows navigation steps: Details, Profile, Scope, Scan settings, and Review. The main area is titled 'Details'.

Details

Provide a name and detailed description of your attachment to help easily find it later.

Name: PR1_007

Description (optional): PR1_007

Buttons at the bottom: Cancel, Back, Next.

Windows taskbar at the bottom:

- Type here to search
- Icons for File Explorer, Task View, Start, Edge, Mail, LinkedIn, Google Chrome, Microsoft Edge, File Explorer, Google Sheets, Google Slides, Google Sheets, Google Slides, Settings, Word.
- System status: 26°C Rain, ENG, 17:03, 27-08-2024.

Screenshot of the IBM Cloud Security and Compliance interface showing the 'Profile' step.

The left sidebar shows navigation steps: Details, Profile, Scope, Scan settings, and Review. The main area is titled 'Profile'.

Profile

Profile: AI Security Guardrails 2.0 (1.0.0)

Parameters

Component: All

Description	Parameters	Component
Check whether Container Registry Vulnerability Advisor scans for critical or high vulnerabilities in the system at least every # day(s)	1	Container Registry
Check whether Virtual Servers for VPC instance has the minimum # interfaces	1	Virtual Server for VPC
Check whether Virtual Servers for VPC instance has all interfaces with IP-spoofing disabled	1	Virtual Server for VPC
Check whether Security Groups for VPC contains no outbound rules in security groups that specify destination IP 8.8.8.8/32	-	-

Buttons at the bottom: Cancel, Back, Next.

Windows taskbar at the bottom:

- Type here to search
- Icons for File Explorer, Task View, Start, Edge, Mail, LinkedIn, Google Chrome, Microsoft Edge, File Explorer, Google Sheets, Google Slides, Google Sheets, Google Slides, Settings, Word.
- System status: 26°C Rain, ENG, 17:03, 27-08-2024.

Security and Compliance | Profiles | AI Security Guardrails 2.0 | Create an attachment

Scope

Target a scope to define the way that your evaluation is conducted.

Scope ⓘ Ganpat-2021-Sem6-rg

Exclude resource groups (optional)

Select exclusions

Target account scope (optional)

Select a target account scope(s)

Cancel Back Next

Type here to search 21162101012_CBA_Y Cloud Object Storage (87) WhatsApp Calling quizzing enti ahmedabad wether. IBM Cloud Search resources and products... Catalog Manage 2716063 - IBM India Pvt Ltd, C/... Back Next

Security and Compliance | Profiles | AI Security Guardrails 2.0 | Create an attachment

Scan settings

Define the details of the evaluation for this scope and profile selection.

Schedule

Select the frequency at which you want to evaluate your selected resources.

Frequency

Every day (recommended)
 Every 7 days
 Every 30 days
 None

Failure notifications

Optionally, you can choose to be notified if evaluations fail during a scan. The alerts can be sent by threshold or individual control.

Notify me

Cancel Back Next

Type here to search 21162101012_CBA_Y Cloud Object Storage (87) WhatsApp Calling quizzing enti ahmedabad wether. IBM Cloud Search resources and products... Catalog Manage 2716063 - IBM India Pvt Ltd, C/... Back Next

The screenshot shows the IBM Cloud interface for Security and Compliance. A sidebar on the left lists steps: Details, Profile, Scope, Scan settings, and Review. The main area is titled "Review" and contains sections for "Details" (Name: PR1_007, Description: optional, PR1_007) and "Profile" (Profile: AI Security Guardrails 2.0, Version: 1.0.0). Below these are "Parameters" and "Cancel" and "Create" buttons. The status bar at the bottom shows a weather forecast for Ahmedabad: 26°C Rain.

It will take time and let the scan finish

The screenshot shows the IBM Cloud interface for Security and Compliance. The main area is titled "AI Security Guardrails 2.0". A yellow box highlights the "Plan" section, which says "Your Trial plan expires in 29 days. To ensure that your scans are not interrupted, upgrade to the Standard plan." with an "Upgrade" button. Below this are tabs for "Overview" and "Attachments (1)". The "Attachments" tab is selected, showing a table with one row:

Name	Environment	Version	Last scanned	Next scan	Status	Updates
PR1_007	IBM Cloud	1.0.0	08/27/2024, 5:05 PM	Scan in progress	Latest version	-

The status bar at the bottom shows a weather forecast for Ahmedabad: 26°C Rain.

An attachment is the connection between a profile and a set of resources that defines the way an evaluation is conducted.

Name	Environment	Version	Last scanned	Next scan	Status	Updates
PR1_007	IBM Cloud	1.0.0	08/27/2024, 5:05 PM	08/28/2024	Latest version	-

After scan completion, check services and security compliances, like here cloud storage bucket should contain firewall for additional security as mentioned in results

Property	Description	Operator	Expected value	Actual value
firewall.allowed_ip	List of allowed originating (source) IP addresses/ranges. The list can contain up to 1000 IPv4 or IPv6 addresses/ranges in CIDR notation.	is_not_empty	[]	

Recommended Remediation:

- This rule might fail if the Cloud Object Storage bucket network access is not configured with a specific firewall IP range.
- Select the Cloud Object Storage resource list.
- Next, select the service instance with your bucket. The Cloud Object Storage console opens.
- Select the bucket that you want to limit access to authorized IP addresses.
- Click the Permissions tab.
- Select Firewall(legacy) from the list of options.
- Click Add to add the list of Authorized IPs.
- Click Add and specify a list of IP addresses in CIDR notation (for example, 192.168.0.0/16, fe80::021b:0/64). Addresses can follow IPv4 or IPv6 standards.
- Review the [IBM Cloud IP ranges](#) to add relevant IPs to the Firewall's Authorized IPs. Add all the IPs that are mentioned for that specific region from where your services access the Cloud Object Storage bucket.
- Click Add.
- The firewall is not enforced until the address is saved in the console. Click Save all to enforce the firewall.

Note: All objects in this bucket are accessible only from those IP addresses that are mentioned in the firewall configuration. If you enable the firewall to allow only specific IP addresses, other internal IBM cloud services might be blocked from accessing this Cloud Object Storage bucket. So, if this bucket is used to store scan results or is connected to any other cloud services, you have to allow access from IBM cloud internal IP addresses to the Cloud Object Storage bucket in the firewall.

Now, it can be solved as mentioned, adding legacy firewall to bucket allowing specific IP addresses or the ranges respectively

The screenshot shows the IBM Cloud Object Storage - IBM instance page. The left sidebar has 'Cloud Object Storage' selected under 'Instances'. The main content area shows the 'Permissions' tab is active. A warning message states: 'Warning: Context-based restrictions are recommended over firewall rules.' Below it, a note says: 'Once the bucket is configured with IP addresses, the data in the bucket can be accessed from the configured IP addresses only.' A 'Learn more' link is present. The bottom part of the screen shows a Windows taskbar with various icons and system status.

The screenshot shows the 'Add IP addresses or Address Ranges' dialog box. It has a text input field labeled 'IP Address' with the placeholder 'Add single or multiple address, comma separated.' Below it is an example: 'Example: 192.168.0.0/16, fe80:021b::/64'. At the bottom are 'Cancel' and 'Add' buttons. The background shows the same IBM Cloud Object Storage interface as the previous screenshot, with a 'Warning' message about context-based restrictions.

Further solutions can be made as per provided steps and sufficient access to resource groups and respective resources

