

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA      Batch - 71

CS Practical 1

**Scenario :** 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 :**

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 1

- 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.

### Screenshots and steps :

#### 1. Create Security and Compliance Centre service and enter region and name

The screenshot shows the IBM Cloud Catalog interface. On the left, there's a sidebar with various service icons. The main area is titled "Security and Compliance Center". It has tabs for "Create" and "About". A dropdown menu for "Select a location" is open, showing "Dallas (us-south)" which is highlighted with a red border. Below it, there's a section for "Select a pricing plan" with two options: "Trial" (free) and "Standard" (\$1.12022414 INR/Evaluation). The "Trial" plan is selected. In the "Configure your resource" section, the "Service name" field contains "YSL\_p1", also highlighted with a red border. To the right, a "Summary" panel shows details: Location: Dallas, Plan: Trial, Service name: YSL\_p1, and Resource group: default. At the bottom, there's a checkbox for accepting license agreements, which is checked, followed by a "Create" button and an "Add to estimate" button.

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 1

## 2. In Control Libraries, go to CIS IBM benchmark library

The screenshot shows the IBM Cloud Security and Compliance interface. The left sidebar is expanded, showing the 'Control libraries' option under the 'Controls' section, which is highlighted with a red box. A red arrow points from this red box down towards the main content area. The main content area displays the 'Control libraries' page with a heading 'Control libraries'. It includes a yellow banner about a trial plan expiring in 29 days, a search bar, and a table listing a single item: 'CIS IBM Cloud Foundations Benchmark v1.1.0 (1.1.0)'. The table has columns for Name, Type, Controls, and Last modified. The 'Name' column shows 'CIS IBM Cloud Foundations Benchmark v1.1.0 (1.1.0)'. The 'Type' column shows 'Predefined'. The 'Controls' column shows '67'. The 'Last modified' column shows '06/25/2024, 7:52 AM'. A red circle highlights the 'CIS IBM' entry in the table. A red arrow also points from the bottom of the sidebar's red box towards the 'CIS IBM' entry in the table.

Name	Type	Controls	Last modified
CIS IBM Cloud Foundations Benchmark v1.1.0 (1.1.0)	Predefined	67	06/25/2024, 7:52 AM

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 1

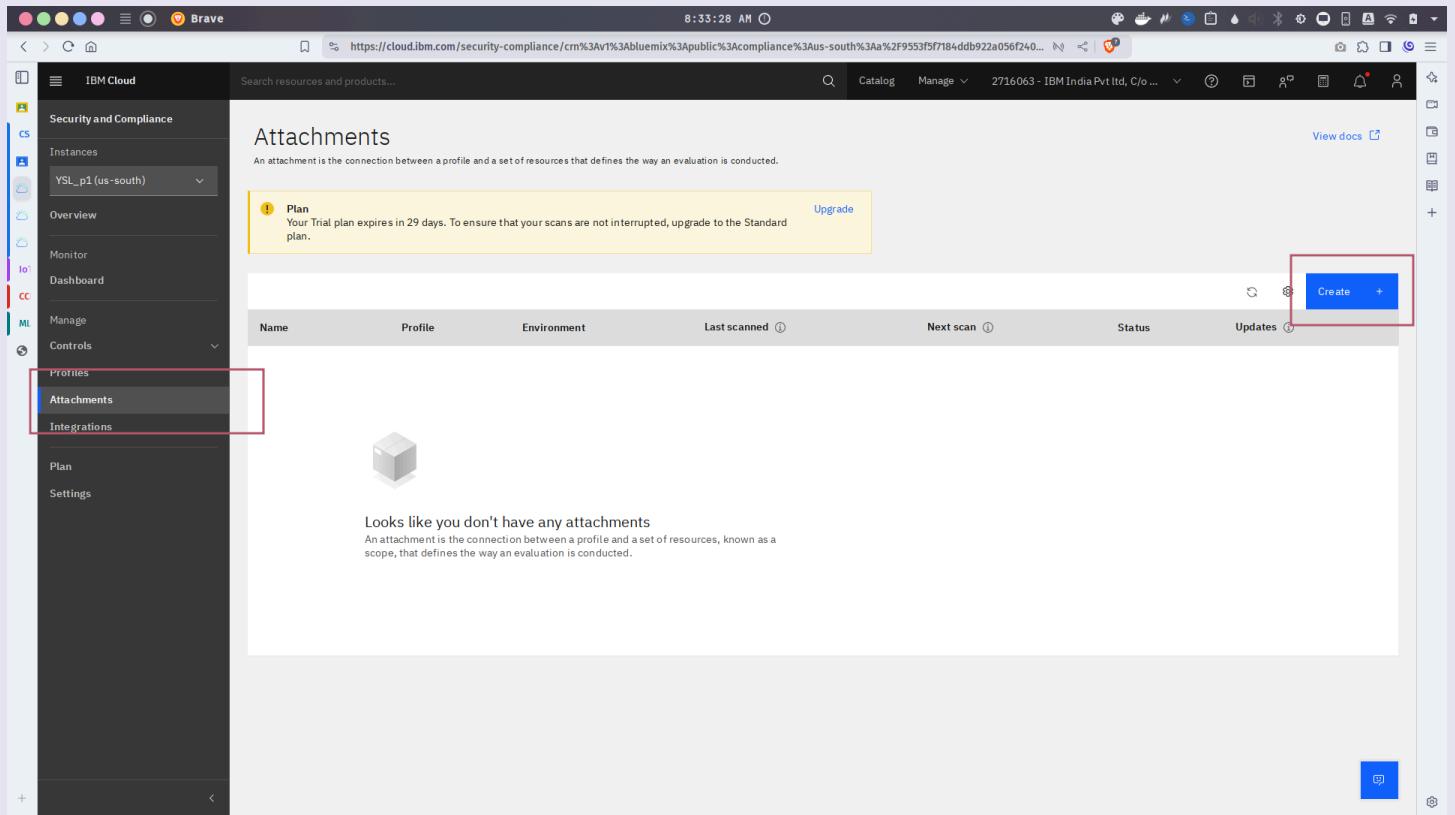
### 3. Here, all controls and benchmarks are visible as per categories, components, specs and controls

The screenshot shows the IBM Cloud Security and Compliance interface. The top navigation bar includes 'IBM Cloud', 'Search resources and products...', 'Catalog', 'Manage', and user information. The main page title is 'CIS IBM Cloud Foundations Benchmark v1.1.0'. A yellow banner at the top left indicates a 'Plan' trial period of 29 days and provides an 'Upgrade' link. Below this, the 'Details' section shows the version '1.1.0', description 'CIS IBM Cloud Foundations Benchmark version 1.1.0', ID '51ca566e-c559-412b-8d64-f05b57044c32', and type 'Predefined'. It also shows the last update date '06/25/2024, 7:52 AM' and a count of 67 controls. At the bottom, a table lists 13 controls grouped by category, with columns for Name, Description, Category, and Specifications. The 'Category' column for all controls is 'Identity and Access Management'.

Name	Description	Category	Specifications
1.4	Restrict user API key creation and service ID creation in the account via IAM roles	Identity and Access Management	2
1.5	Ensure no owner account API key exists	Identity and Access Management	1
1.6	Ensure compliance with IBM Cloud password requirements	Identity and Access Management	8
1.10	Ensure contact email is valid	Identity and Access Management	1
1.11	Ensure contact phone number is valid	Identity and Access Management	1
1.12	Ensure IAM users are members of access groups and IAM policies are assigned only to access groups	Identity and Access Management	1
1.13	Ensure a support access group has been created to manage incidents with IBM Support	Identity and Access Management	1

**Name - Yash Lakhtariya**  
**Enrollment number - 21162101012**  
**Branch - CBA      Batch - 71**  
**CS Practical 1**

#### 4. Now in service home, visit attachments and add one



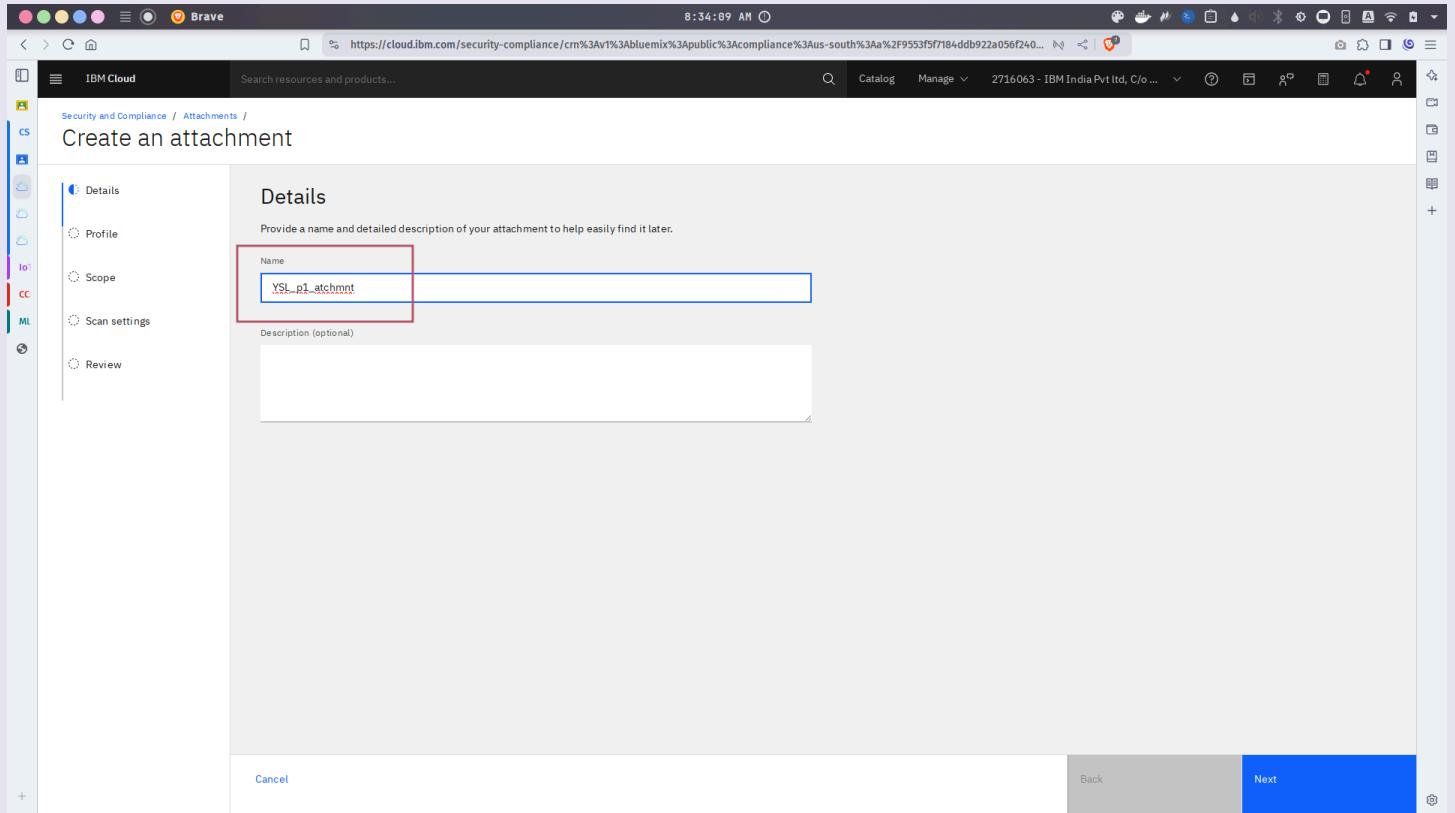
The screenshot shows the IBM Cloud Security & Compliance service interface. The left sidebar has a dark theme with a navigation menu:

- IBM Cloud
- Security and Compliance
- Instances (dropdown: YSL\_p1 (us-south))
- Overview
- Monitor
- Dashboard
- Manage
- Controls
- Profiles (highlighted with a red box)
- Attachments (highlighted with a red box)
- Integrations
- Plan
- Settings

The main content area is titled "Attachments". It displays a message: "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 callout box with a warning icon: "Plan Your Trial plan expires in 29 days. To ensure that your scans are not interrupted, upgrade to the Standard plan." with a "Upgrade" link. A table header is shown with columns: Name, Profile, Environment, Last scanned, Next scan, Status, and Updates. A large "Create +" button is located at the top right of the table area. The message "Looks like you don't have any attachments" is displayed below the table.

**Name - Yash Lakhtariya**  
**Enrollment number - 21162101012**  
**Branch - CBA      Batch - 71**  
**CS Practical 1**

## 5. Enter name and proceed further



The screenshot shows a web browser window for IBM Cloud, specifically the Security and Compliance section. The URL is https://cloud.ibm.com/security-compliance/crm%3Av1%3Abluemix%3Apublic%3Aus-south%3Aa%2F9553f5f7184ddb922a056f240... . The page title is "Create an attachment". On the left, there's a sidebar with various icons and sections like "IBM Cloud", "Search resources and products...", "Catalog", "Manage", and user info. The main area has a sidebar with steps: "Details", "Profile", "Scope", "Scan settings", "Review", and "Next". The "Details" step is active, showing a "Name" field containing "YSL\_p1.atchmnt" which is highlighted with a red box. Below it is a "Description (optional)" field. At the bottom, there are "Cancel", "Back", and a large blue "Next" button.

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA      Batch - 71

CS Practical 1

6. Now, the storage is needed to proceed, Cloud Object Bucket can be used also here

The screenshot shows the IBM Cloud interface for Security and Compliance. The user is in the 'Attachments' section, specifically creating a new attachment. The left sidebar has a 'Profile' tab selected. The main area is titled 'Profile' and displays a message: 'Select a profile to define the way that your evaluation is conducted.' Below this is a warning about 'Storage configuration missing' and a 'Connect' button. A dropdown menu shows 'AI ICT Guardrails (1.0.0)' selected. The bottom section is titled 'Parameters' and lists several configuration items under 'Toolchain', 'Container Registry', and 'Virtual Server for VPC'. There are 'Back' and 'Next' buttons at the bottom right.

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
Check whether Virtual Servers for VPC instance has all interfaces with IP-spoofing disabled	1	Virtual Server for VPC

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 1

## 7. Authorize the service instance

The screenshot shows the IBM Cloud Security and Compliance Center interface. On the left, there's a sidebar with various icons and a main panel titled "Create an attachment". The main panel has tabs: "Details" (selected), "Profile", "Scope", "Scan settings", and "Review". Under "Profile", it says "Select a profile to define the way that your evaluation is run" and shows "AIICT Guardrails (1.0.0)". Below that is a "Parameters" section with a table. The table has columns "Description" and "Value". There are three rows, each with a dropdown arrow icon. The first row's value is "Check whether Toolchain is configured only". The second row's value is "Check whether Container Registry Vulnerabilities are present". The third row's value is "Check whether Virtual Servers for VPC instances are configured". At the bottom of the main panel are "Cancel" and "Connect" buttons.

**Connect storage**

Connect a Cloud Object Storage bucket to store your evaluation results. As a best practice, it is recommended that you use a bucket that is located in the same region in which your data is processed.

Not sure if your bucket will work? [Learn more about bucket requirements.](#)

**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**

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 1

## 8. Select the object storage instance

The screenshot shows the IBM Cloud Security and Compliance interface. On the left, there's a sidebar with various service icons and a main panel titled "Create an attachment". The main panel has tabs for "Profile", "Parameters", and "Review". The "Profile" tab is active, showing a "Storage configuration missing" message and a "Connect" button. The "Parameters" tab lists several check items under "Description". On the right, a modal window titled "Authorize service to service access for Security and Compliance" is open. It asks to "Select a target service" and lists "Cloud Object Storage" as the selected service. Below it, there are dropdowns for "Region" (set to "All regions"), "serviceInstance" (set to "string equals" and "Cloud Object Storage-2v (f56f5908-9e6e...)" highlighted with a red box), "resource" (set to "string equals"), "resourceType" (set to "string equals"), "Prefix" (set to "string equals"), "Delimiter" (set to "string equals"), and "Path" (set to "string equals"). At the bottom of the modal are "Cancel" and "Review" buttons.

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 1

## 9. Allow write access to the security service instance

The screenshot shows the 'Create an attachment' interface in the IBM Cloud Security and Compliance center. The left sidebar lists steps: Details, Profile (selected), Scope, Scan settings, and Review. The main area has two tabs: 'Profile' and 'Parameters'. The 'Profile' tab shows a 'Storage configuration missing' message and a 'Connect' button. The 'Parameters' tab lists components: All, Toolchain, Container Registry, and Virtual Servers. The 'Access' section at the bottom allows selecting a role for the source service. The 'Writer' checkbox is checked and highlighted with a red box. A tooltip explains: 'As a Writer, one can create/modify/delete buckets. In addition, one can upload and download the objects in the bucket.' The bottom navigation bar includes 'Cancel' and 'Review' buttons.

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 1

The screenshot shows the IBM Cloud Security and Compliance interface. A modal window titled "Review service to service authorization for Security and Compliance" is open. It displays the target service as "Cloud Object Storage" and the role as "Writer". A red arrow points from the "Assign" button at the bottom right of the modal to the "Assign" button at the bottom right of the main interface window.

Profile

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

Storage configuration

To allow Security and Compliance to access your service, create a connection. Learn more

Profile

AI IICT Guardrails (1.0.0)

Parameters

Component: All

Description

Check whether Toolchain is configured only

Check whether Container Registry Vulnerability

Check whether Virtual Servers for VPC insta

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.

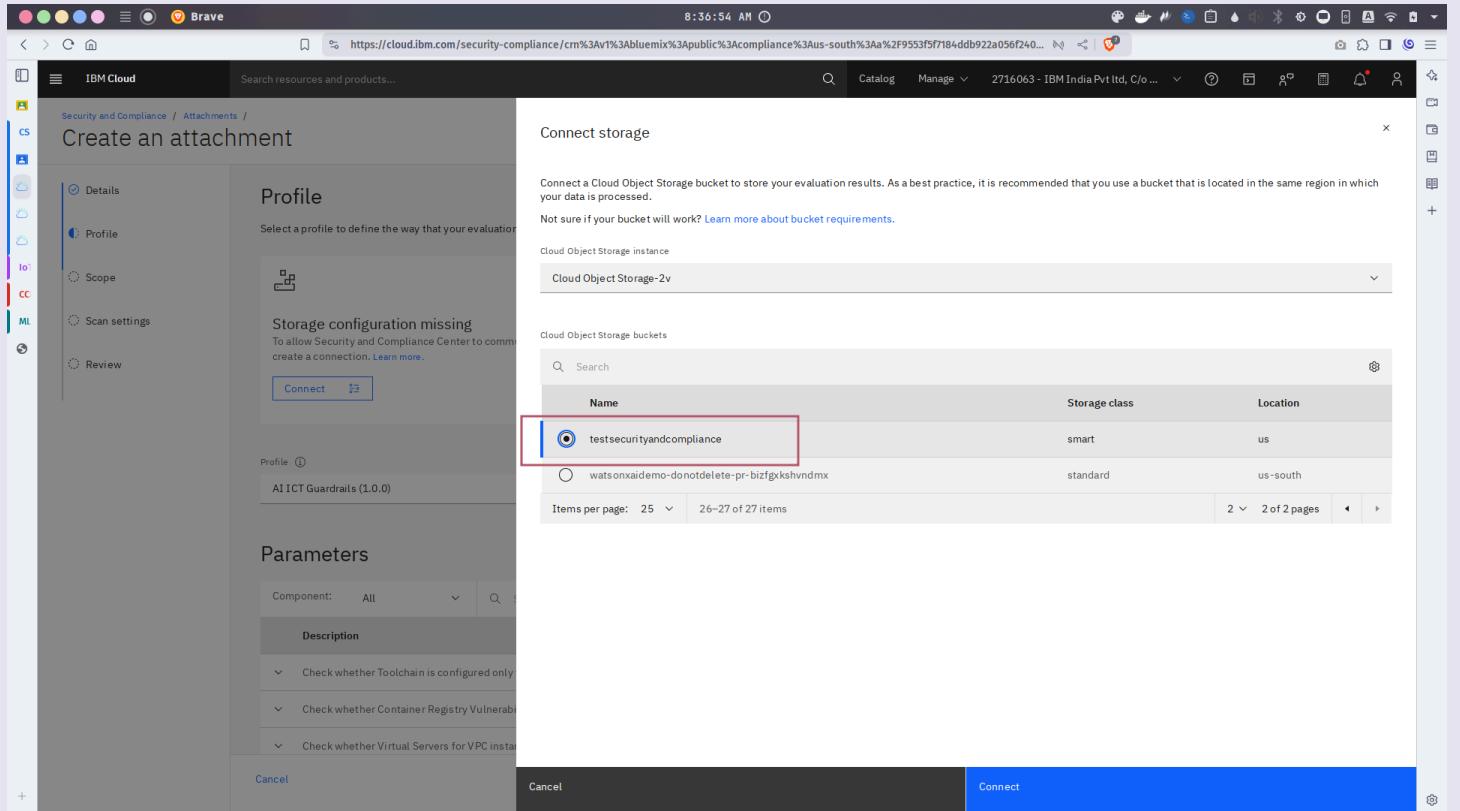
Assign

Assign

Review

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 1

10. After assigning the role, now select the bucket to be used here



The screenshot shows the IBM Cloud interface with a specific modal window for connecting storage. The main background page is titled 'Create an attachment' under 'Security and Compliance / Attachments /'. It includes tabs for 'Details', 'Profile', 'Scope', 'Scan settings', and 'Review'. The 'Profile' tab is active, showing a 'Storage configuration missing' message and a 'Connect' button. The modal window, titled 'Connect storage', contains instructions to connect a Cloud Object Storage bucket. It lists 'Cloud Object Storage instance' as 'Cloud Object Storage-2v' and shows a table of 'Cloud Object Storage buckets'. The table has columns for 'Name', 'Storage class', and 'Location'. Two buckets are listed: 'testsecurityandcompliance' (selected) and 'watsonxairdemo-donotdelete-pr-bizfgxkshvndmx'. Both have 'smart' storage class and 'us' location. The 'testsecurityandcompliance' row is highlighted with a red border. At the bottom of the modal are 'Cancel' and 'Connect' buttons.

Name	Storage class	Location
testsecurityandcompliance	smart	us
watsonxairdemo-donotdelete-pr-bizfgxkshvndmx	standard	us-south

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 1

## 11. Select the scope of this service instance

The screenshot shows a web browser window for the IBM Cloud Security and Compliance service. The URL is https://cloud.ibm.com/security-compliance/crm%3Av1%3Abluemix%3Apublic%3Acompliance%3Aus-south%3Aa%2F9553f5f7184ddb922a056f240... The page title is "Create an attachment". On the left, there's a sidebar with icons for CS, ML, AI, and CC, followed by a vertical list of steps: Details, Profile, Scope (which is selected), Scan settings, and Review. The main content area is titled "Scope" with the sub-instruction "Target a scope to define the way that your evaluation is conducted.". It contains three input fields: "Scope" (containing "Ganpat-2021-Sem6-rg" with a red box around it), "Exclude resource groups (optional)" (with a "Select exclusions" dropdown), and "Target account scope (optional)" (with a "Select a target account scope(s)" dropdown). At the bottom, there are "Cancel", "Back", and "Next" buttons, with "Next" being highlighted in blue.

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA      Batch - 71

CS Practical 1

12. Scan settings should be everyday as recommended here to avoid intrusion and threats or any failure due to weak security

The screenshot shows the 'Create an attachment' page in the IBM Cloud Security and Compliance interface. On the left, a sidebar lists steps: Details, Profile, Scope, Scan settings (which is selected and highlighted in blue), and Review. The main panel is titled 'Scan settings' and contains the following sections:

- Scan settings**: A sub-section under 'Details'.
- Schedule**: A sub-section under 'Scan settings'. It asks to select the frequency for evaluation. The 'Frequency' section contains four options:
  - Every day (recommended)
  - Every 7 days
  - Every 30 days
  - None
- Failure notifications**: A sub-section under 'Scan settings'. It says optional failure notifications can be sent by threshold or individual control. A 'Notify me' toggle switch is shown, which is turned on (indicated by a grey circle).

At the bottom right of the main panel are 'Cancel', 'Back', and 'Next' buttons. The 'Next' button is highlighted in blue.

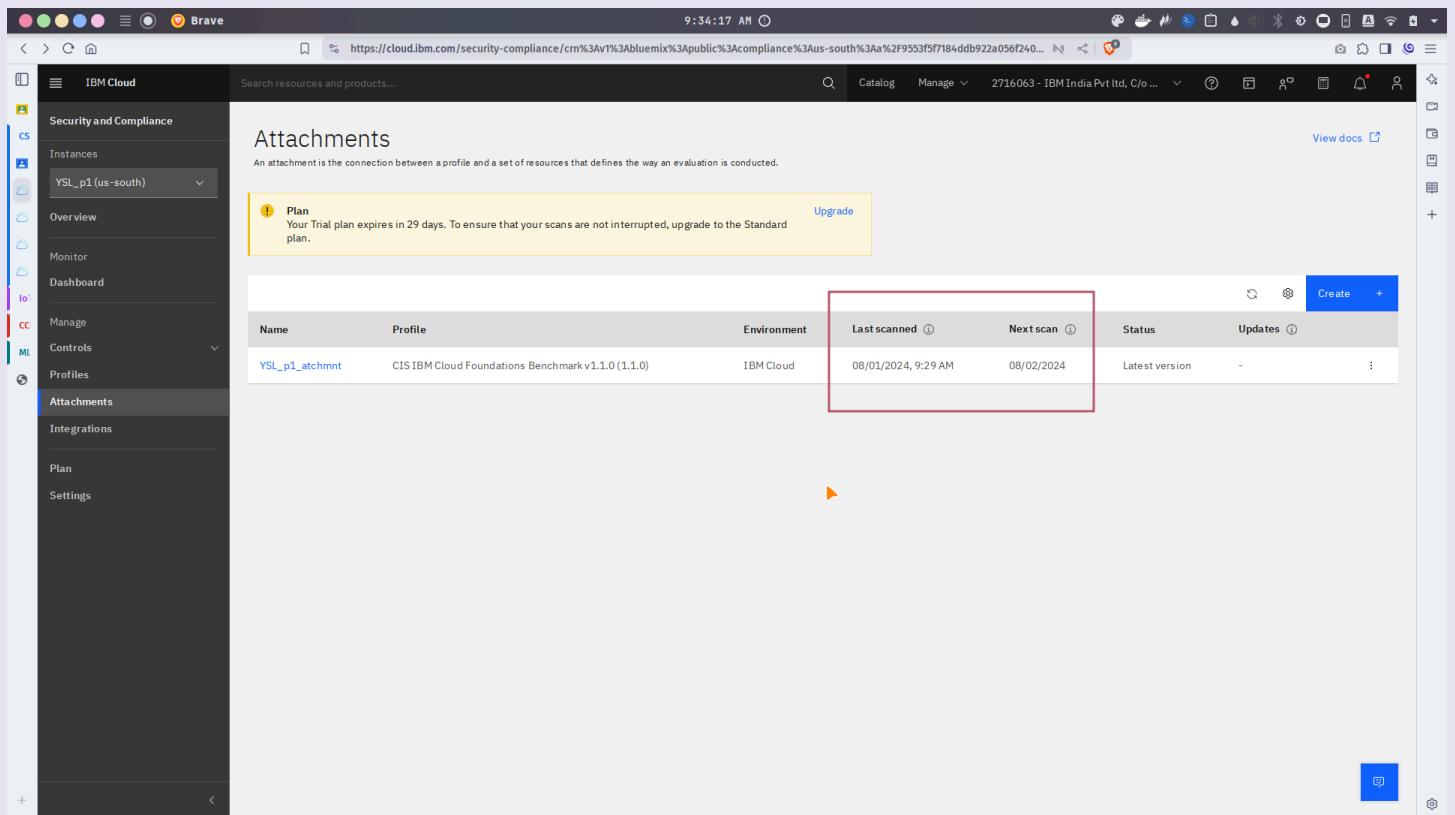
Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 1

### 13. Review settings and create attachment

The screenshot shows the 'Create an attachment' interface in the IBM Cloud Security and Compliance section. The left sidebar lists steps: Details, Profile, Scope, Scan settings, and Review. The 'Review' step is selected. The main area is titled 'Review' and contains a note: 'Before you begin evaluating your resources, review your settings and ensure that all of your configurations are correct for your targeted scope.' Below this are three sections: 'Details', 'Profile', and 'Parameters'. The 'Details' section shows a name 'YSL\_p1\_atchmnt' and an optional description. The 'Profile' section shows a profile 'AI ICT Guardrails' and version '1.0.0'. The 'Parameters' section lists four items under 'Description': 'Check whether Toolchain is configured only with the allowed integration tools', 'Check whether Container Registry Vulnerability Advisor scans for critical or high vulnerabilities in the system at least every # day(s)', 'Check whether Virtual Servers for VPC instance has all interfaces with IP-spoofing disabled', and 'Check whether Security Groups for VPC contains no outbound rules in security groups that specify destination IP 8.8.8.8/32 to DNS port'. The 'Component' column for these items is 'Toolchain', 'Container Registry', 'Virtual Server for VPC', and 'Security Group for VPC' respectively. A red arrow points from the top right towards the 'Create' button. The bottom right corner of the 'Create' button has a small red hand icon pointing to it.

**Name - Yash Lakhtariya**  
**Enrollment number - 21162101012**  
**Branch - CBA      Batch - 71**  
**CS Practical 1**

**14. After scan is completed the next scan will be after 24 hours**



The screenshot shows the IBM Cloud Security & Compliance interface in a web browser. The left sidebar navigation includes: IBM Cloud, Security and Compliance (selected), Instances (YSL\_p1 (us-south)), Overview, Monitor, Dashboard, Manage, Controls, Profiles, **Attachments** (selected), Integrations, Plan, and Settings. The main content area is titled "Attachments" and contains a message: "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 callout box with a warning icon: "Plan Your Trial plan expires in 29 days. To ensure that your scans are not interrupted, upgrade to the Standard plan." with a "Upgrade" button. A table lists attachments with columns: Name, Profile, Environment, Last scanned, Next scan, Status, and Updates. One row is shown: YSL\_p1\_atchmnt, CIS IBM Cloud Foundations Benchmark v1.1.0 (1.1.0), IBM Cloud, 08/01/2024, 9:29 AM, 08/02/2024, Latest version, -. The "Last scanned" and "Next scan" columns are highlighted with a red border.

Name	Profile	Environment	Last scanned	Next scan	Status	Updates
YSL_p1_atchmnt	CIS IBM Cloud Foundations Benchmark v1.1.0 (1.1.0)	IBM Cloud	08/01/2024, 9:29 AM	08/02/2024	Latest version	-

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 1

15. Click on the attachment and click the profile details

The screenshot shows the IBM Cloud Security & Compliance interface in a web browser. The left sidebar has 'Attachments' selected. The main area displays an 'Attachments' list with one item: 'YSL\_p1 (us-south)'. A modal window titled 'Attachment details' is open over the list. The modal contains the following information:

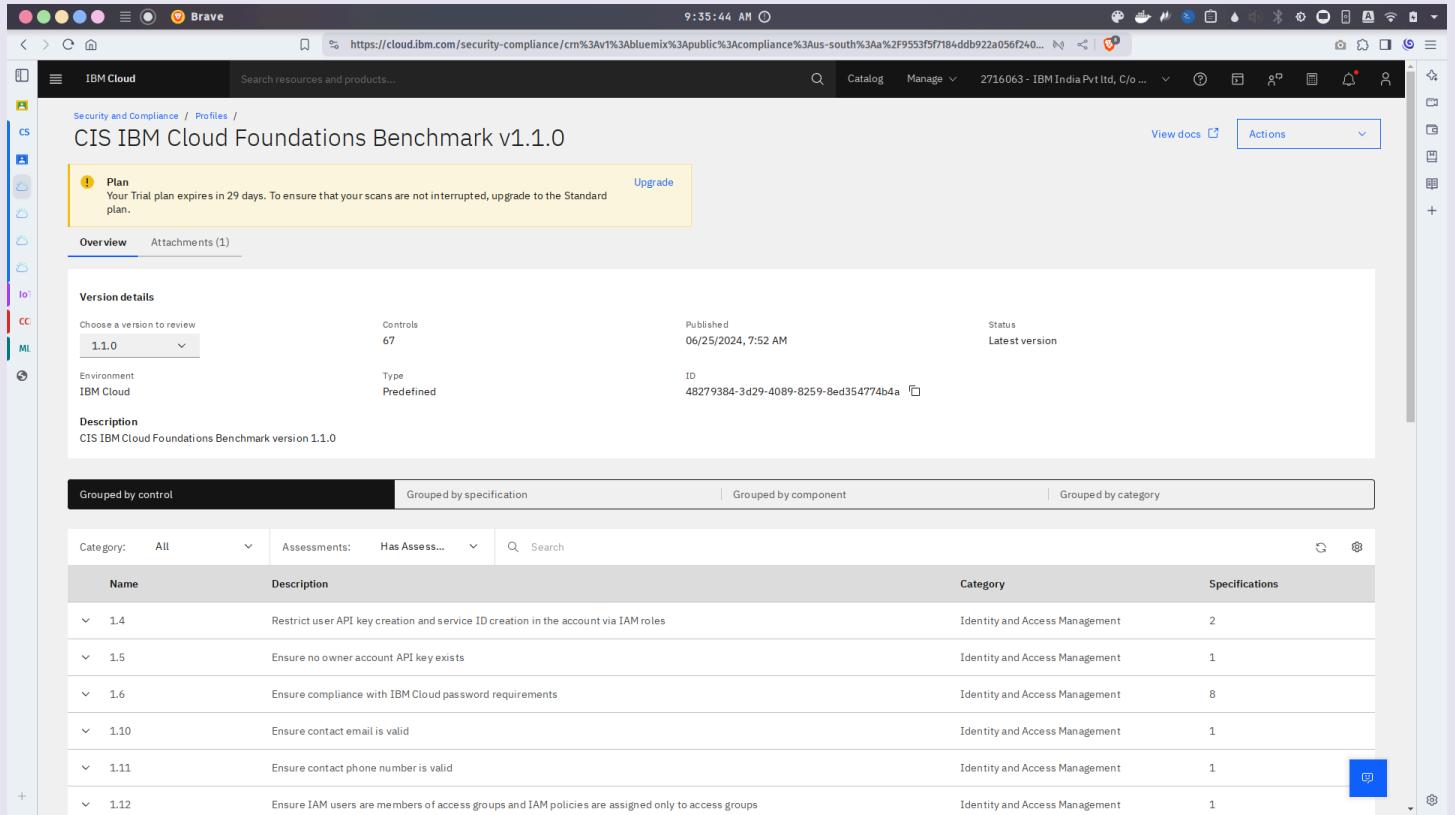
Name	Profile	Environment	Last scanned
YSL_p1_atchmnt	CIS IBM Cloud Foundations Benchmark v1.1.0 (1.1.0)	IBM Cloud	08/01/2024, 9:29

On the right side of the modal, there are three tabs: 'Scope', 'Scan settings', and 'Parameters'. The 'Scope' tab is active and shows the following details:

- Environment: IBM Cloud
- Scope: Ganpat-2021-Sem6-rg
- Type: Resource group
- Exclusions: None

**Name - Yash Lakhtariya**  
**Enrollment number - 21162101012**  
**Branch - CBA      Batch - 71**  
**CS Practical 1**

## 16. All controls are visible here

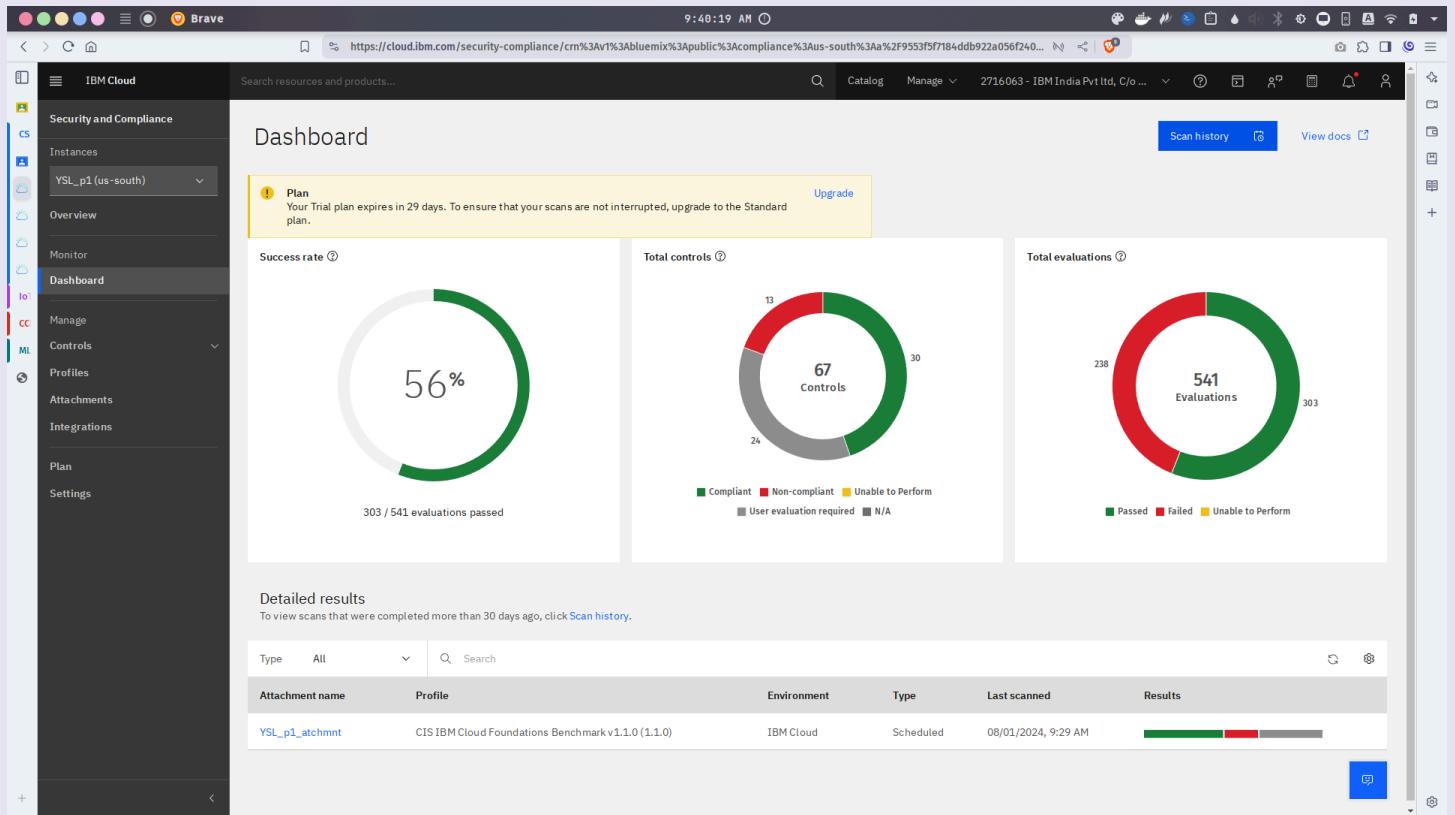


The screenshot shows the IBM Cloud Security and Compliance interface. The URL is https://cloud.ibm.com/security-compliance/crm%3Av1%3Abluemix%3Apublic%3Acompliance%3Aus-south%3Aa%2F955f5f7184ddb922a056f240... The page title is CIS IBM Cloud Foundations Benchmark v1.1.0. The main content area displays version details: Version 1.1.0, Controls 67, Published 06/25/2024, 7:52 AM, Status Latest version. It also shows the environment as IBM Cloud and the type as Predefined. Below this, there is a table of controls grouped by control, specification, component, or category. The table has columns for Name, Description, Category, and Specifications. The controls listed are:

Name	Description	Category	Specifications
1.4	Restrict user API key creation and service ID creation in the account via IAM roles	Identity and Access Management	2
1.5	Ensure no owner account API key exists	Identity and Access Management	1
1.6	Ensure compliance with IBM Cloud password requirements	Identity and Access Management	8
1.10	Ensure contact email is valid	Identity and Access Management	1
1.11	Ensure contact phone number is valid	Identity and Access Management	1
1.12	Ensure IAM users are members of access groups and IAM policies are assigned only to access groups	Identity and Access Management	1

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 1

17. In dashboard on service home, the results are mentioned

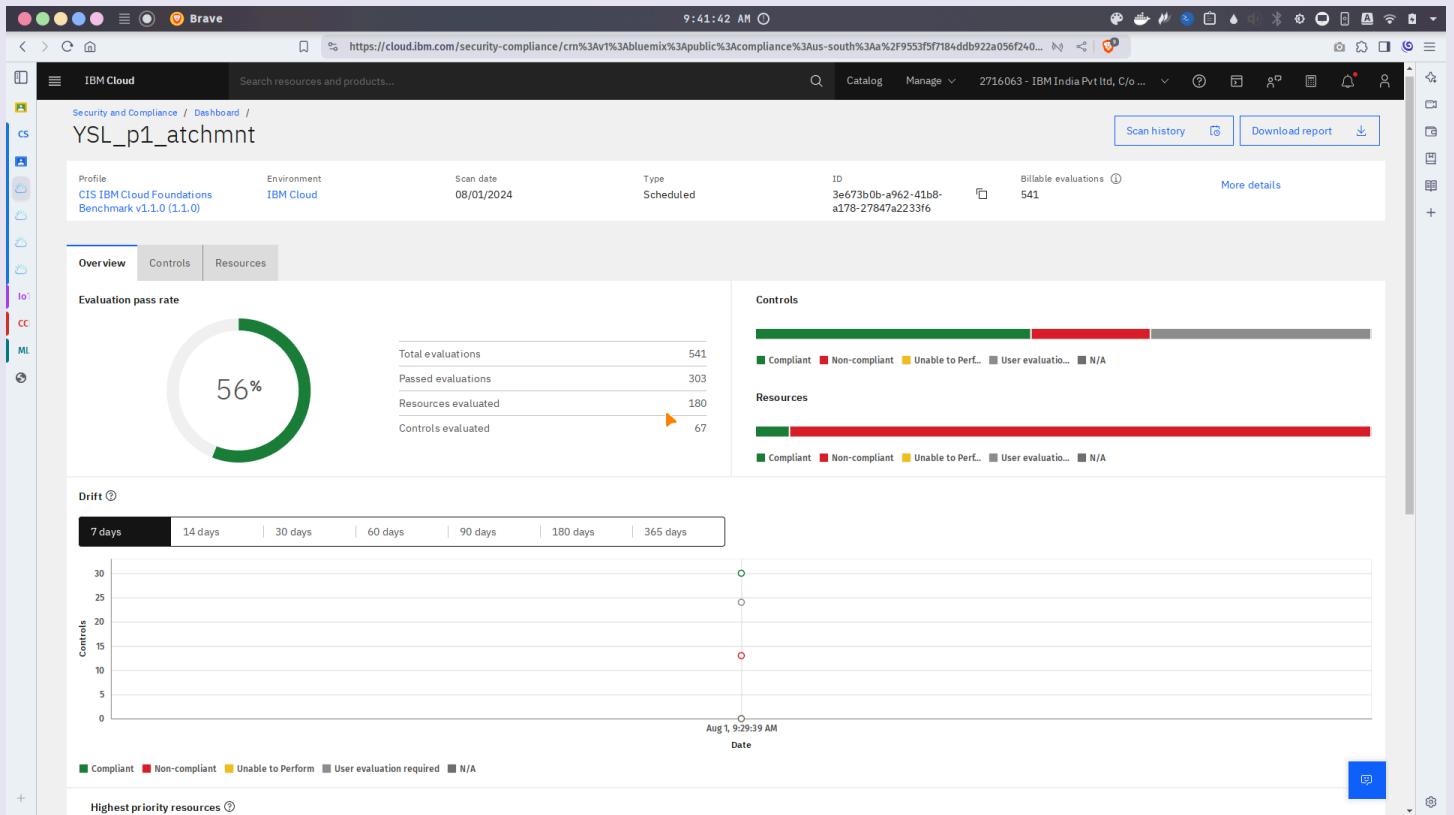


Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 1

## 18. Click on the attachment to check its detailed results

The screenshot shows the IBM Cloud Security & Compliance dashboard. On the left, a sidebar menu is visible with options like 'Instances', 'Overview', 'Monitor', 'Dashboard' (which is selected), 'Manage', 'Controls', 'Profiles', 'Attachments', 'Integrations', 'Plan', and 'Settings'. The main area displays three circular dashboards: 'Success rate' (56%, 303 / 541 evaluations passed), 'Total controls' (67 Controls, 13 Non-compliant, 24 User evaluation required, 30 N/A), and 'Total evaluations' (541 Evaluations, 238 Failed, 303 Passed). Below these is a section titled 'Detailed results' with a table. The table has columns: Type (All), Attachment name (YSL\_p1\_attachment, highlighted with a red border), Profile (CIS IBM Cloud Foundations Benchmark v1.1.0 (1.1.0)), Environment (IBM Cloud), Type (Scheduled), Last scanned (08/01/2024, 9:29 AM), and Results (a bar chart showing mostly green 'Passed' status with a few red 'Failed' segments). A search bar and a 'Scan history' button are also present.

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 1



Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA      Batch - 71

CS Practical 1

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

The screenshot shows the IBM Cloud Security and Compliance interface. The top navigation bar includes 'IBM Cloud', 'Search resources and products...', 'Catalog', 'Manage', and a user profile. The main page displays a scan report for a CIS IBM Cloud Foundations Benchmark v1.1.0 (1.1.0) profile. The 'Controls' tab is active, showing a list of findings:

Name	Description	Category	Specifications	Evaluation
1.16	Ensure IAM does not allow public access to Cloud Object Storage	Identity and Access Management	1	<div style="width: 100px; height: 10px; background-color: red;"></div>
2.1.1.1	Ensure Cloud Object Storage encryption is done with customer managed keys	Storage	1	<div style="width: 100px; height: 10px; background-color: red;"></div>

Under the '2.1.1.1' finding, there is a detailed view of specifications:

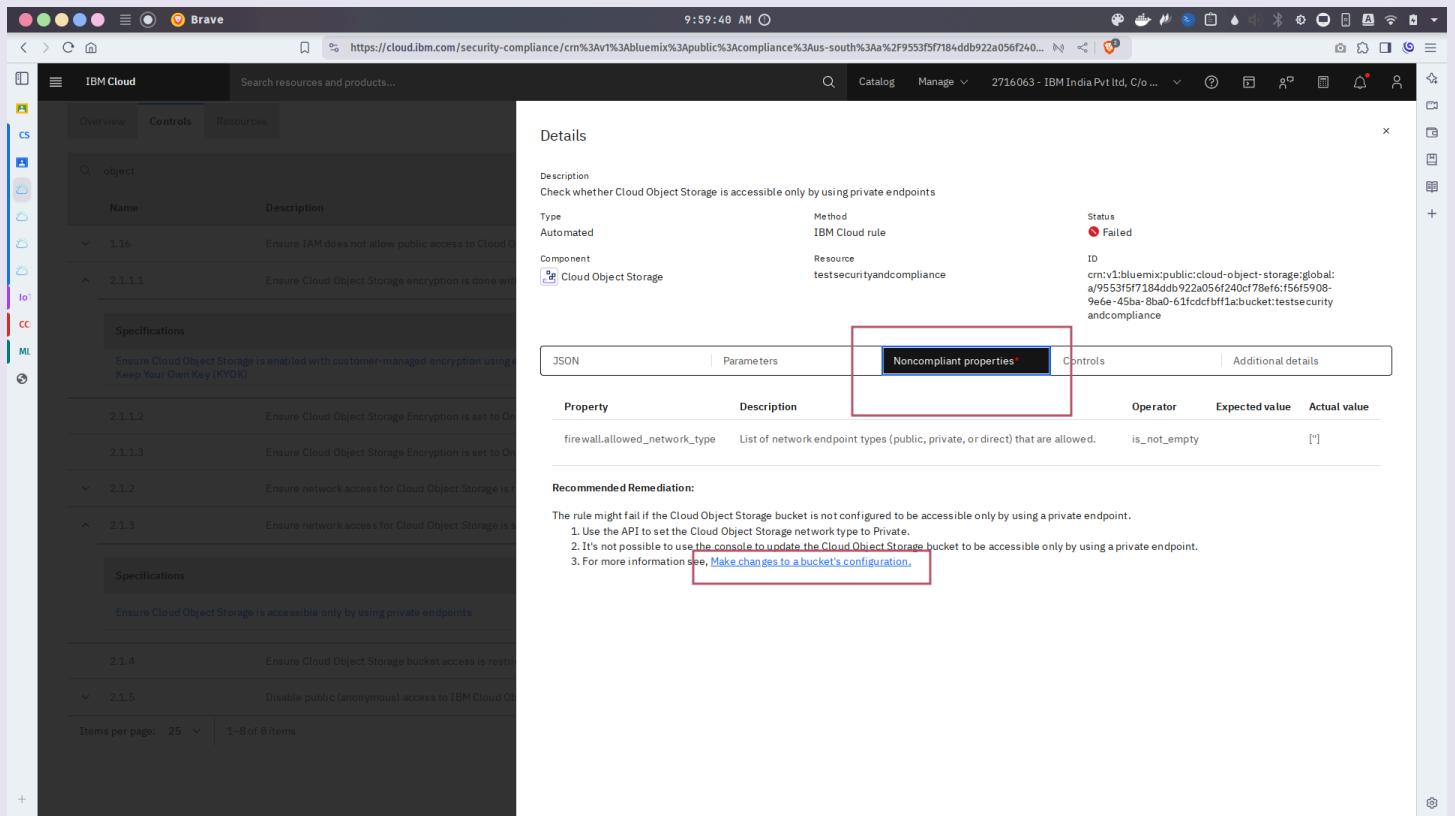
Specifications	Component	Environment	Status	Compliant	Non-compliant	Unable to Perform
Ensure Cloud Object Storage is enabled with customer-managed encryption using either Bring Your Own Key (BYOK) or Keep Your Own Key (KYOK)	Cloud Object Storage	IBM Cloud	<span style="color: red;">Non-compliant</span>	-	<span style="color: red;">32</span>	-

Other findings listed include:

- 2.1.1.2: Ensure Cloud Object Storage Encryption is set to On with BYOK (Status: Compliant, 0 non-compliant)
- 2.1.1.3: Ensure Cloud Object Storage Encryption is set to On with KYOK (Status: Compliant, 0 non-compliant)
- 2.1.2: Ensure network access for Cloud Object Storage is restricted to specific IP range (Status: Non-compliant, 1 non-compliant)
- 2.1.3: Ensure network access for Cloud Object Storage is set to be exposed only on private endpoints (Status: Non-compliant, 1 non-compliant)

**Name - Yash Lakhtariya**  
**Enrollment number - 21162101012**  
**Branch - CBA      Batch - 71**  
**CS Practical 1**

**20. 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 Compliance interface. On the left, there's a sidebar with various icons and a search bar. The main area has tabs for 'Overview', 'Controls' (which is selected), and 'Resources'. The 'Controls' tab shows a list of rules under the 'object' category. One rule, 'Ensure IAM does not allow public access to Cloud Object Storage', is expanded, showing its specifications. Another rule, 'Ensure Cloud Object Storage encryption is done with customer-managed encryption using Keep Your Own Key (KYOK)', is also visible. On the right, a detailed view of a specific rule is shown. The rule is titled 'Check whether Cloud Object Storage is accessible only by using private endpoints'. It is categorized as 'Automated' with 'IBM Cloud rule' as the method. The status is 'Failed'. The ID of the rule is 'cm:v1:bluemix:public:cloud-object-storage:global:a/955315f7184ddb922a056f1240cf78ef6f56f5908-9e6a-45ba-8ba0-61fcdfbf12abucket:testsecurityandcompliance'. Below this, there's a table with columns for 'Property', 'Description', 'Operator', 'Expected value', and 'Actual value'. A red box highlights the 'Noncompliant properties' tab in the table header. At the bottom, there's a section for 'Recommended Remediation' with three steps: 1. Use the API to set the Cloud Object Storage network type to Private. 2. It's not possible to use the console to update the Cloud Object Storage bucket to be accessible only by using a private endpoint. 3. For more information see, [Make changes to a bucket's configuration](#).

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA      Batch - 71

CS Practical 1

21. 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 & Compliance interface. The left sidebar has 'Attachments' selected. The main area is titled 'Attachments' with a sub-instruction: 'An attachment is the connection between a profile and a set of resources that defines the way an evaluation is conducted.' A yellow callout box for 'Plan' says 'Your Trial plan expires in 29 days. To ensure that your scans are not interrupted, upgrade to the Standard plan.' An 'Upgrade' button is in the top right of the callout. The table below lists one attachment:

Name	Profile	Environment	Last scanned	Next scan	Status	Updates
YSL_p1_attachmnt	CIS IBM Cloud Foundations Benchmark v1.1.0 (1.1.0)	IBM Cloud	08/01/2024, 9:29 AM	08/02/2024	Latest version	-

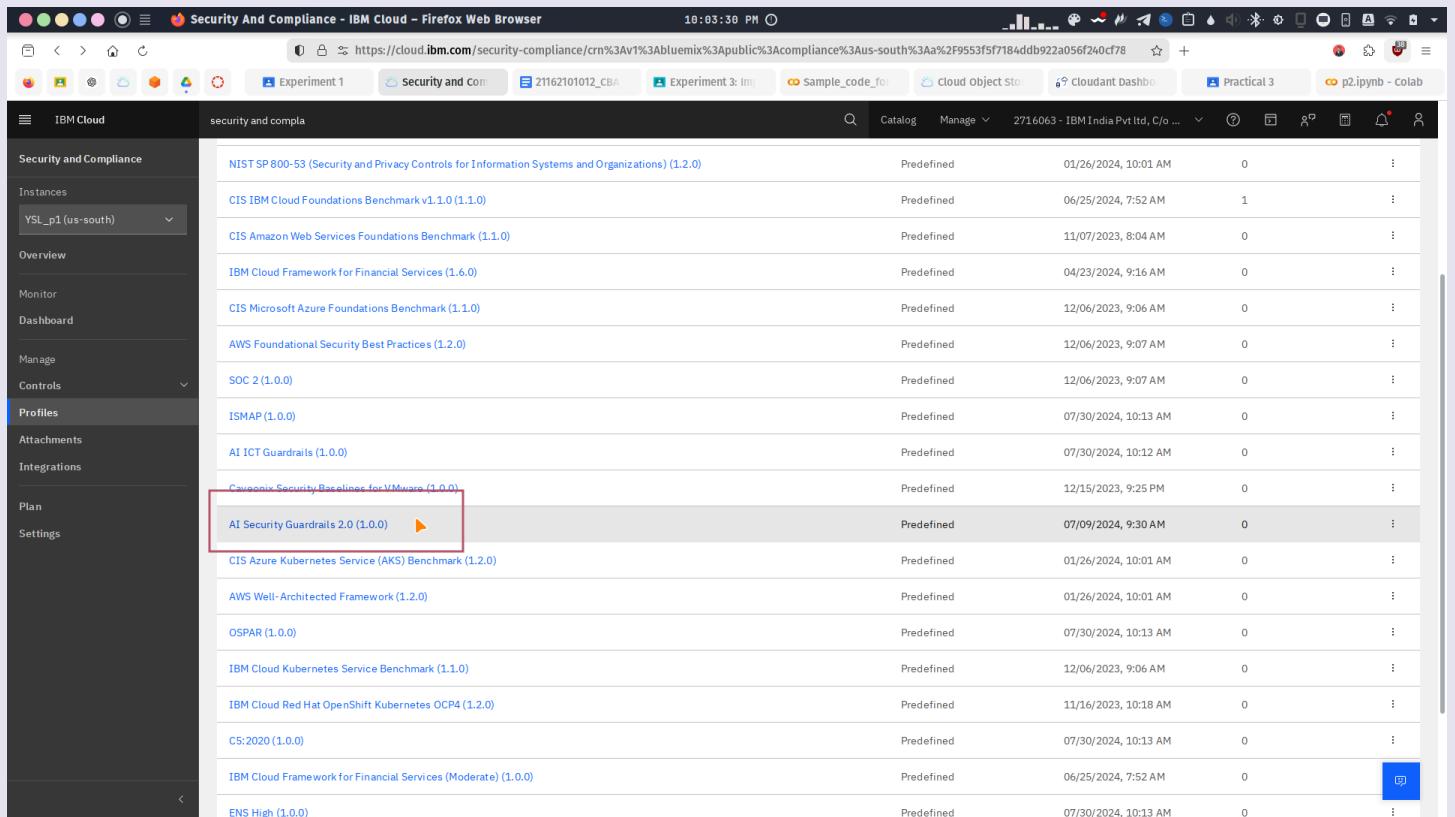
A context menu is open over the first row of the table, with the 'Run scan' option highlighted by a red box and a cursor pointing at it.

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 1

**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.**

## 22. Visit AI Security Guardrails profile



The screenshot shows the IBM Cloud Security and Compliance interface in a Firefox browser. The left sidebar is titled 'IBM Cloud' and includes sections for 'Security and Compliance', 'Instances' (set to 'YSL\_p1 (us-south)'), 'Overview', 'Monitor', 'Dashboard', 'Manage', 'Controls', 'Profiles' (which is selected), 'Attachments', 'Integrations', 'Plan', and 'Settings'. The main content area is titled 'security and complia' and shows a table of compliance profiles. The table has columns for 'Name', 'Type', 'Last Update', 'Issues', and 'Actions'. One row, 'AI Security Guardrails 2.0 (1.0.0)', is highlighted with a red box and a yellow play button icon. Other profiles listed include NIST SP 800-53, CIS IBM Cloud Foundations Benchmark v1.1.0, CIS Amazon Web Services Foundations Benchmark, IBM Cloud Framework for Financial Services, CIS Microsoft Azure Foundations Benchmark, AWS Foundational Security Best Practices, SOC 2 (1.0.0), ISMAP (1.0.0), AI ICT Guardrails (1.0.0), Cisconix Security Baseline for VMware, CIS Azure Kubernetes Service (AKS) Benchmark, AWS Well-Architected Framework, OSPIR (1.0.0), IBM Cloud Kubernetes Service Benchmark, IBM Cloud Red Hat OpenShift Kubernetes OCP4, C5:2020, IBM Cloud Framework for Financial Services (Moderate), and ENS High.

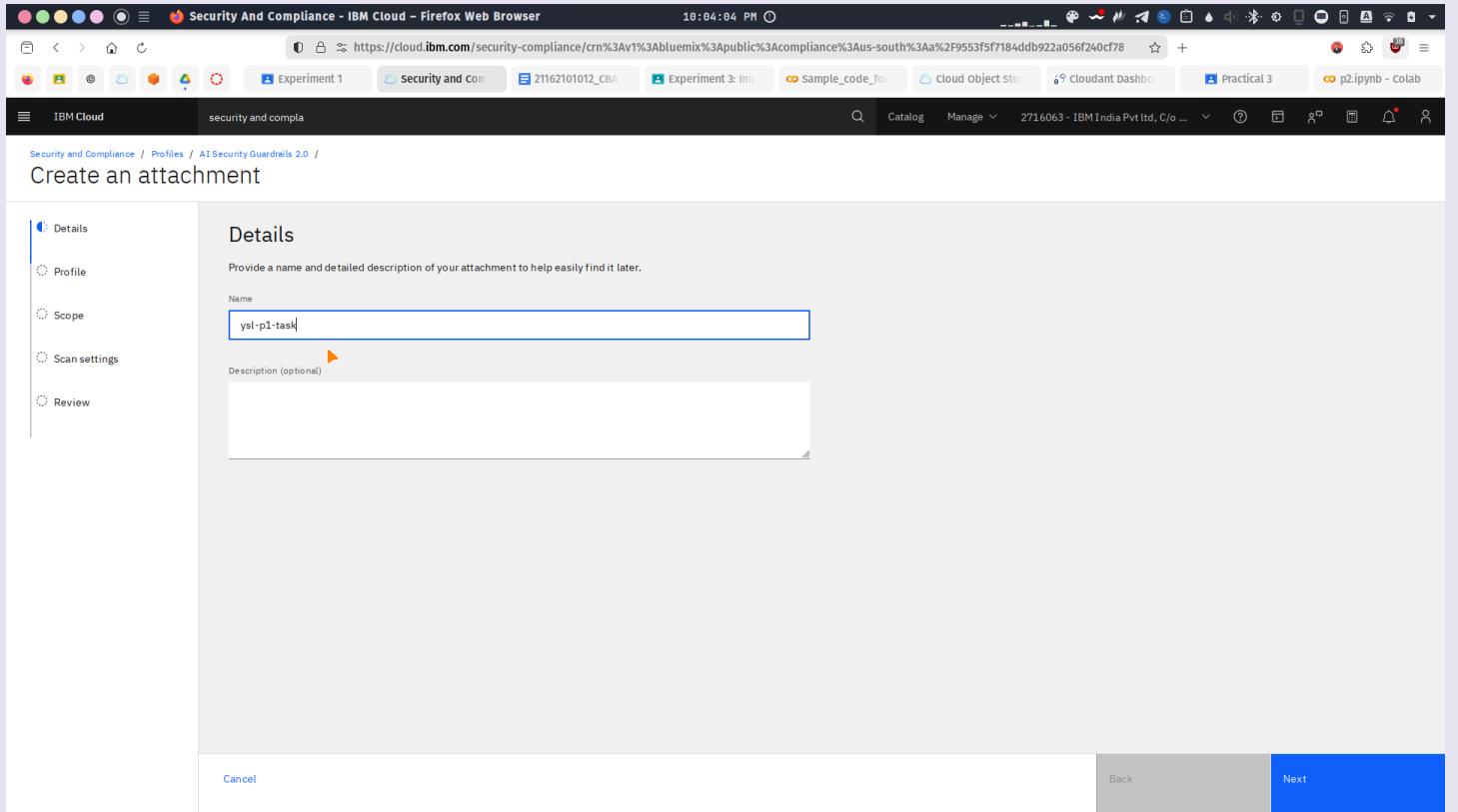
Name	Type	Last Update	Issues	Actions
NIST SP 800-53 (Security and Privacy Controls for Information Systems and Organizations) (1.2.0)	Predefined	01/26/2024, 10:01 AM	0	⋮
CIS IBM Cloud Foundations Benchmark v1.1.0 (1.1.0)	Predefined	06/25/2024, 7:52 AM	1	⋮
CIS Amazon Web Services Foundations Benchmark (1.1.0)	Predefined	11/07/2023, 8:04 AM	0	⋮
IBM Cloud Framework for Financial Services (1.6.0)	Predefined	04/23/2024, 9:16 AM	0	⋮
CIS Microsoft Azure Foundations Benchmark (1.1.0)	Predefined	12/06/2023, 9:06 AM	0	⋮
AWS Foundational Security Best Practices (1.2.0)	Predefined	12/06/2023, 9:07 AM	0	⋮
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	⋮
AI ICT Guardrails (1.0.0)	Predefined	07/30/2024, 10:12 AM	0	⋮
Cisconix Security Baseline for VMware (1.0.0)	Predefined	12/15/2023, 9:25 PM	0	⋮
<b>AI Security Guardrails 2.0 (1.0.0)</b>	Predefined	07/09/2024, 9:30 AM	0	⋮
CIS Azure Kubernetes Service (AKS) Benchmark (1.2.0)	Predefined	01/26/2024, 10:01 AM	0	⋮
AWS Well-Architected Framework (1.2.0)	Predefined	01/26/2024, 10:01 AM	0	⋮
OSPIR (1.0.0)	Predefined	07/30/2024, 10:13 AM	0	⋮
IBM Cloud Kubernetes Service Benchmark (1.1.0)	Predefined	12/06/2023, 9:06 AM	0	⋮
IBM Cloud Red Hat OpenShift Kubernetes OCP4 (1.2.0)	Predefined	11/16/2023, 10:18 AM	0	⋮
C5:2020 (1.0.0)	Predefined	07/30/2024, 10:13 AM	0	⋮
IBM Cloud Framework for Financial Services (Moderate) (1.0.0)	Predefined	06/25/2024, 7:52 AM	0	⋮
ENS High (1.0.0)	Predefined	07/30/2024, 10:13 AM	0	⋮

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 1

## 23. Create new attachment

The screenshot shows the IBM Cloud Security And Compliance interface in a Firefox browser. The URL is <https://cloud.ibm.com/security-compliance/crn%3Av1%3Abluemix%3Apublic%3Acompliance%3Aus-south%3Aa%2F9553f5f7184ddb922a056f240cf78>. The page title is "Security And Compliance - IBM Cloud - Firefox Web Browser". The top navigation bar includes links for Catalog, Manage, and a user profile. The main content area is titled "AI Security Guardrails 2.0". A yellow banner at the top left says "Plan" and "Your Trial plan expires in 16 days. To ensure that your scans are not interrupted, upgrade to the Standard plan." with an "Upgrade" button. Below this, there are two numbered 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). A large "Attachments (0)" section follows, featuring a "Create" button with a plus sign, which is highlighted with a red box. At the bottom, a message states "Looks like you don't have any attachments" and provides a definition of what an attachment is.

**Name - Yash Lakhtariya**  
**Enrollment number - 21162101012**  
**Branch - CBA      Batch - 71**  
**CS Practical 1**



The screenshot shows a Firefox browser window titled "Security And Compliance - IBM Cloud - Firefox Web Browser". The URL is <https://cloud.ibm.com/security-compliance/crn%3Av1%3Abuemix%3Apublic%3Acompliance%3Aus-south%3Aa%2F9553f5f7184dd922a056f240cf78>. The page is titled "Create an attachment". On the left, there is a sidebar with tabs: "Details" (selected), "Profile", "Scope", "Scan settings", and "Review". The main area is titled "Details" and contains a "Name" field with the value "ysl-p1-task" and a "Description (optional)" field which is empty. At the bottom, there are "Cancel", "Back", and "Next" buttons. The "Next" button is highlighted in blue.

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 1

## 24. Select all parameters and set scan scope and frequency

The screenshot shows a Firefox browser window titled "Security And Compliance - IBM Cloud - Firefox Web Browser". The URL is <https://cloud.ibm.com/security-compliance/crn%3Av1%3Abluemix%3Apublic%3Acompliance%3Aus-south%3Aa%2F9553f5f7184dd922a056f240cf78>. The page displays the "Create an attachment" step of the "AI Security Guardrails 2.0" profile creation process.

**Profile:** AI Security Guardrails 2.0 (1.0.0)

**Parameters:**

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 to DNS port	1	Security Group for VPC
Check whether Virtual Private Cloud (VPC) security groups have inbound ports that are open only to permitted IP addresses	1	Security Group for VPC
Check whether Virtual Private Cloud (VPC) security groups have outbound ports that are open only to permitted IP addresses	1	Security Group for VPC
Check whether at least # Virtual Private Cloud (VPC)s have been created	1	Virtual Private Cloud
Check whether at least # instances of Transit Gateway have been created	1	transit

**Buttons:** Cancel, Back, Next

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 1

Security And Compliance - IBM Cloud - Firefox Web Browser 10:04:39 PM

https://cloud.ibm.com/security-compliance/crn%3Av1%3Abluemix%3Apublic%3Acompliance%3Aus-south%3Aa%2F9553f5f7184ddb922a056f240cf78

Experiment 1 Security and Com... 21162101012\_CBA Experiment 3: Im... Sample\_code\_fo... Cloud Object Sto... Cloudant Dashbo... Practical 3 p2.ipynb - colab

IBM Cloud security and compla

Security and Compliance / Profiles / AI Security Guardrails 2.0 / 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

Security And Compliance - IBM Cloud - Firefox Web Browser 10:04:39 PM

https://cloud.ibm.com/security-compliance/crn%3Av1%3Abluemix%3Apublic%3Acompliance%3Aus-south%3Aa%2F9553f5f7184ddb922a056f240cf78

Experiment 1 Security and Com... 21162101012\_CBA Experiment 3: Im... sample\_code\_fo... Cloud Object Sto... Cloudant Dashbo... Practical 3 p2.ipynb - colab

IBM Cloud security and compla

Security and Compliance / Profiles / AI Security Guardrails 2.0 / 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

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 1

## 25. It will take time and let the scan finish

The screenshot shows the IBM Cloud Security and Compliance interface in a Firefox browser. The URL is <https://cloud.ibm.com/security-compliance/crn%3Av1%3Abluemix%3Apublic%3Acompliance%3Aus-south%3Aa%2F9553f5f7184ddb922a056f240cf78>. The page title is "Security And Compliance - IBM Cloud - Firefox Web Browser". The top navigation bar includes links for Experiment 1, Security and Complia..., Experiment 3, Sample\_code\_10, Cloud Object Sto..., Cloudant Dashbo..., Practical 3, and p2.ipynb - colab. The main content area shows the "AI Security Guardrails 2.0" profile. A yellow banner at the top left says "Plan" and "Your Trial plan expires in 16 days. To ensure that your scans are not interrupted, upgrade to the Standard plan." with an "Upgrade" button. Below this, there are tabs for "Overview" and "Attachments (1)". The "Attachments" tab is selected, showing a table with one row. The table columns are Name, Environment, Version, Last scanned, Next scan, Status, and Updates. The row contains: Name - ysl-p1-task, Environment - IBM Cloud, Version - 1.0.0, Last scanned - 08/14/2024, 10:05 PM, Next scan - "Scan in progress" (highlighted with a red box), Status - Latest version, and Updates - -. There is a "Create" button in the top right corner of the attachments table.

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 1

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

The screenshot shows the IBM Cloud Security And Compliance interface in a Firefox browser. The URL is https://cloud.ibm.com/security-compliance/crn%3Av1%3Abuemix%3Apublic%3Acompliance%3Aus-south%3Aa%2F9553f5f7184ddb922a056f240cf78. The page displays a list of resources under 'IBM Cloud' and focuses on an 'Assessment' for a bucket named 'testsecurity'. A specific rule is highlighted in red:

**Description:** Check whether Cloud Object Storage network access is restricted to a specific IP range.

**Type:** Automated

**Method:** IBM Cloud rule

**Component:** Cloud Object Storage

**Resource:** testsecurity

**Status:** Failed

**ID:** crn:1:bluemix:public:cloud-object-storage:global:9553f5f7184ddb922a056f240cf78:6f04d634bf-1c6f-4bc2-b7cd-7622a0e6ddeb0:7bucket:testsecurity

The 'Noncompliant properties\*' tab is selected in the JSON table, showing a single entry:

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.

1. Select Storage to view your resource list.
2. Next, select the service instance with your bucket. The Cloud Object Storage console opens.
3. Select the bucket that you want to limit access to authorized IP addresses.
4. Click the Permissions tab.
5. Select Firewall(legacy) from the list of options.
6. Click Add to add the list of Authorized IPs.
7. Click Add and specify a list of IP addresses in CIDR notation (for example, 192.168.0.0/16, fe80:021b::/64). Addresses can follow IPv4 or IPv6 standards.
8. 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.
9. Click Add.
10. 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.

Name - Yash Lakhtariya

Enrollment number - 21162101012

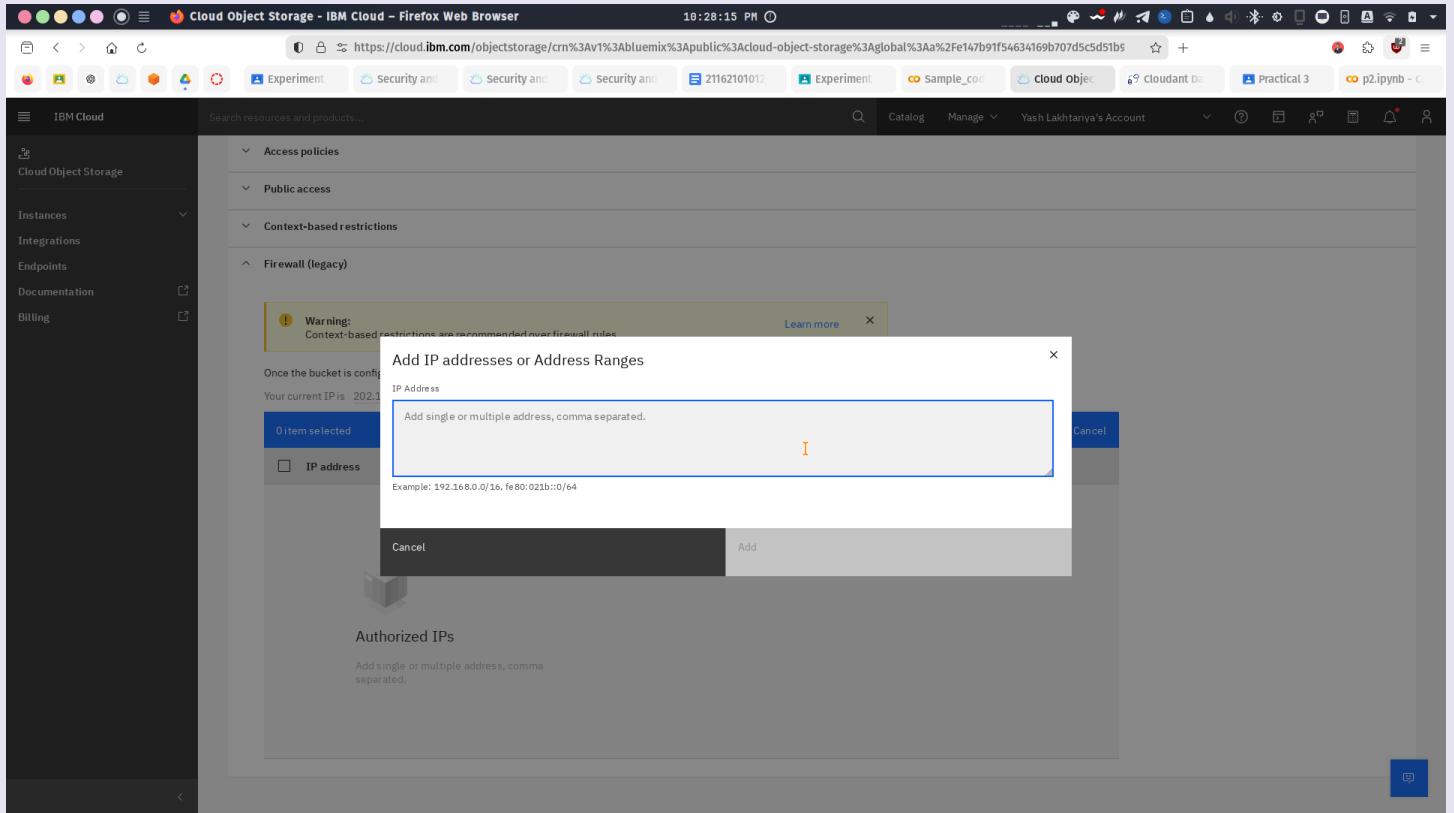
Branch - CBA      Batch - 71

CS Practical 1

27. 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 interface in a Firefox browser. The URL is https://cloud.ibm.com/objectstorage/crn%3Av1%3Abuemix%3Apublic%3Acloud-object-storage%3Aglobal%3Aa%2Fe147b91f54634169b707d5c5d51b5. The page displays the 'Cloud Object Storage' access policies for a specific bucket. A red box highlights the 'Firewall (legacy)' section under 'Context-based restrictions'. A yellow warning box states: 'Warning: Context-based restrictions are recommended over firewall rules.' Below this, a message says: 'Once the bucket is configured with IP addresses, the data in the bucket can be accessed from the configured IP addresses only.' It also shows the current IP address as 202.131.113.234. A red box encloses the 'Add' button and search bar for entering IP addresses. The bottom section is labeled 'Authorized IPs' with a placeholder text: 'Add single or multiple address, comma separated.'

**Name - Yash Lakhtariya**  
**Enrollment number - 21162101012**  
**Branch - CBA      Batch - 71**  
**CS Practical 1**



The screenshot shows the IBM Cloud Object Storage interface in a Firefox browser. The URL is https://cloud.ibm.com/objectstorage/crn%3Av1%3Abuemix%3Apublic%3Acloud-object-storage%3Aglobal%3Aa%2Fe147b91f54634169b707d5c5d51b5. The page displays a warning about context-based restrictions being recommended over firewall rules. A modal dialog box titled 'Add IP addresses or Address Ranges' is open, prompting the user to add single or multiple addresses separated by commas. The example provided is 192.168.0.0/16, fe80:021b::/64. There are 'Cancel' and 'Add' buttons at the bottom of the dialog.

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