

- Purpose of this Folder

# Purpose of this Folder

This folder should contain a fully working project. This will be added to the reviewer toolkit for reviewers to use.

- Step 1 & 2 >

- Submission 1:

- enterprise-analyst-policy:

Edit [enterprise-analyst-policy](#)

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

[Visual editor](#) [JSON](#) [Import managed policy](#)

```

1 {
2     "Version": "2012-10-17",
3     "Statement": [
4         {
5             "Condition": {
6                 "StringEquals": {
7                     "s3:ExistingObjectTag/Role": "analyst"
8                 }
9             },
10            "Action": [
11                "s3>ListObjects",
12                "s3>ListObjectsV2",
13                "s3:GetObject",
14                "s3:GetObjects"
15            ],
16            "Resource": [
17                "arn:aws:s3:::legacy-developer-bucket-706648619117/*"
18            ],
19            "Effect": "Allow",
20            "Sid": "S3AnalystGetObjectByRole"
21        },
22        {
23            "Condition": {
24                "StringEquals": {
25                    "s3:RequestObjectTag/Role": "analyst"
26                }
27            },
28            "Action": [
29                "s3>PutObject"
30            ],
31            "Resource": [
32                "arn:aws:s3:::legacy-developer-bucket-706648619117/*"
33            ],
34            "Effect": "Allow",
35            "Sid": "S3AnalystUploadObjectsByRole"
36        },
37        {
38            "Action": [
39                "s3>ListAllMyBuckets",
40                "s3>ListBucket"
41            ],
42            "Resource": "*",
43            "Effect": "Allow",
44            "Sid": "S3BucketReadAccess"
45        },
46        {
47            "Condition": {
48                "StringEquals": {
49                    "s3:ExistingObjectTag/Stage": "ObfuscatedReportReady"
50                }
51            },
52            "Action": [
53                "s3>ListObjects",
54                "s3>ListObjectsV2",
55                "s3:GetObject",
56                "s3:GetObjects"
57            ],
58            "Resource": [
59                "arn:aws:s3:::analytics-report-bucket-706648619117",
60                "arn:aws:s3:::analytics-report-bucket-706648619117/*"
61            ],
62            "Effect": "Allow",
63            "Sid": "AnalyticsReportBucketAccess"
64        }
65    ]
66 }
```

[Security: 0](#) [Errors: 6](#) [Warnings: 0](#) [Suggestions: 0](#)

Character count: 969 of 6,144. [Cancel](#) [Review policy](#)

## ■ enterprise-developer-policy:

### Edit enterprise-developer-policy

1 2

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor

JSON

Import managed policy

```
1 {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Condition": {  
6                 "StringEquals": {  
7                     "s3:ExistingObjectTag/Role": "developer"  
8                 }  
9             },  
10            "Action": [  
11                "s3>ListObjects",  
12                "s3>ListObjectsV2",  
13                "s3GetObject",  
14                "s3GetObjects"  
15            ],  
16            "Resource": [  
17                "arn:aws:s3:::legacy-developer-bucket-706648619117/*"  
18            ],  
19            "Effect": "Allow",  
20            "Sid": "S3DeveloperGetObjectsByRole"  
21        },  
22        {  
23            "Condition": {  
24                "StringEquals": {  
25                    "s3:RequestObjectTag/Role": "developer"  
26                }  
27            },  
28            "Action": [  
29                "s3PutObject*"  
30            ],  
31            "Resource": [  
32                "arn:aws:s3:::legacy-developer-bucket-706648619117/*"  
33            ],  
34            "Effect": "Allow",  
35            "Sid": "S3DeveloperUploadObjectsByRole"  
36        },  
37        {  
38            "Action": [  
39                "s3>ListAllMyBuckets",  
40                "s3ListBucket"  
41            ],  
42            "Resource": "*",  
43            "Effect": "Allow",  
44            "Sid": "S3BucketReadAccess"  
45        },  
46        {  
47            "Action": [  
48                "ec2Describe*"  
49            ],  
50            "Resource": "*",  
51            "Effect": "Allow",  
52            "Sid": "Ec2MonitorAccess"  
53        },  
54        {  
55            "Action": [  
56                "autoscalingDescribe*",  
57                "cloudwatchDescribe*",  
58                "cloudwatchGet*",  
59                "cloudwatchList*",  
60                "snsGet*",  
61                "snsList"  
62            ],  
63            "Resource": "*",  
64            "Effect": "Allow",  
65            "Sid": "CloudWatchReadAccess"  
66        }  
}
```

🛡 Security: 0

✖ Errors: 3

⚠ Warnings: 0

💡 Suggestions: 0

Character count: 908 of 6,144.

Cancel

Review policy

## ■ enterprise-finance-policy:

Policies > enterprise-finance-policy

**Summary**

Policy ARN arn:aws:iam::706648619117:policy/SecurityAMCourse2/enterprise-finance-policy [Edit](#)

Description

**Permissions** **Policy usage** Tags Policy versions Access Advisor

**Policy summary** [JSON](#) [Edit policy](#)

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Action": [
6         "aws-portal:ViewBilling"
7       ],
8       "Resource": "*",
9       "Effect": "Allow",
10      "Sid": "BillingForAccountAccess"
11    }
12  ]
13 }
```

## ■ enterprise-restrictions-policy:

### Edit enterprise-restrictions-policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

**Visual editor** **JSON** [Import managed policy](#)

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Condition": {
6         "StringNotEquals": {
7           "aws:RequestedRegion": [
8             "us-east-1",
9             "us-east-2",
10            "us-west-1",
11            "us-west-2"
12          ]
13        }
14      },
15      "Resource": "*",
16      "Effect": "Deny",
17      "NotAction": [
18        "cloudfront:*",
19        "iam:*",
20        "route53:*",
21        "support:*"
22      ],
23      "Sid": "DenyAllOutsideRequestedRegions"
24    }
25  ]
26 }
```

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

Character count: 277 of 6,144. [Cancel](#) [Review policy](#)

- Submission 2:

## ■ enterprise-analyst-role:

**Summary**

Creation date February 05, 2023, 09:36 (UTC+01:00)	ARN arn:aws:iam::706648619117:role/enterprise-analyst-role	Link to switch roles in console <a href="https://signin.aws.amazon.com/switchrole?roleName=enterprise-analyst-role&amp;account=706648619117">https://signin.aws.amazon.com/switchrole?roleName=enterprise-analyst-role&amp;account=706648619117</a>
Last activity None	Maximum session duration 1 hour	

**Permissions**

Permissions policies (2) Info  
You can attach up to 10 managed policies.

Policy name	Type	Description
enterprise-analyst-policy	Customer managed	
enterprise-restrictions-policy	Customer managed	

## ■ enterprise-developer-role:

**Summary**

Creation date February 05, 2023, 09:36 (UTC+01:00)	ARN arn:aws:iam::706648619117:role/enterprise-developer-role	Link to switch roles in console <a href="https://signin.aws.amazon.com/switchrole?roleName=enterprise-developer-role&amp;account=706648619117">https://signin.aws.amazon.com/switchrole?roleName=enterprise-developer-role&amp;account=706648619117</a>
Last activity None	Maximum session duration 1 hour	

**Permissions**

Permissions policies (2) Info  
You can attach up to 10 managed policies.

Policy name	Type	Description
enterprise-developer-policy	Customer managed	
enterprise-restrictions-policy	Customer managed	

## ■ enterprise-finance-role:

**Summary**

Creation date February 05, 2023, 09:36 (UTC+01:00)	ARN arn:aws:iam::706648619117:role/enterprise-finance-role	Link to switch roles in console <a href="https://signin.aws.amazon.com/switchrole?roleName=enterprise-finance-role&amp;account=706648619117">https://signin.aws.amazon.com/switchrole?roleName=enterprise-finance-role&amp;account=706648619117</a>
Last activity None	Maximum session duration 1 hour	

**Permissions**

Permissions policies (2) Info  
You can attach up to 10 managed policies.

Policy name	Type	Description
enterprise-finance-policy	Customer managed	
enterprise-restrictions-policy	Customer managed	

- Step 3 & 4 >

- Submission 3:

## ■ non\_obfuscated.txt:

The screenshot shows the AWS S3 console with the URL [https://s3.console.aws.amazon.com/s3/object/analytics-report-bucket-706648619117?region=us-east-1&prefix=non\\_obfuscated.txt](https://s3.console.aws.amazon.com/s3/object/analytics-report-bucket-706648619117?region=us-east-1&prefix=non_obfuscated.txt). The object overview section displays the XML content of the file:

```

<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>13KGJY8Y30T6W5RX</RequestId>
<HostId>1OKXU1@nLuas9pghd13SVWR96zMQ0UjReWzzfyTeFn9utX0Vi2kikm5o0HzdN+mzErcN64k=</HostId>
</Error>

```

## ■ obfuscated.txt:

The screenshot shows the AWS S3 console with the URL <https://s3.console.aws.amazon.com/s3/object/analytics-report-bucket-706648619117?region=us-east-1&prefix=obfuscated.txt>. The object overview section is empty.

## ■ analyst.txt:

The screenshot shows the AWS S3 upload status page with the URL <https://s3.console.aws.amazon.com/s3/upload/legacy-developer-bucket-706648619117?region=us-east-1>. The summary table shows the upload details:

Destination	Succeeded	Failed
<a href="#">s3://legacy-developer-bucket-706648619117</a>	1 file, 0 B (0%)	0 files, 0 B (0%)

The files and folders section shows the uploaded file:

Name	Folder	Type	Size	Status	Error
analyst.txt	-	text/plain	0 B	<span style="color: green;">Succeeded</span>	-

## ■ developer.txt:

The screenshot shows the AWS S3 console interface. At the top, a green banner indicates "Upload succeeded". Below it, the "Upload: status" page displays a summary table with one row: "Destination s3://legacy-developer-bucket-706648619117" and "Succeeded 1 file, 0 B (0%)". Below the summary is a table titled "Files and folders (1 Total, 0 B)" containing a single entry: "developer.txt" (text/plain, 0 B, Succeeded). The bottom of the page includes standard AWS navigation links like Feedback, Language, and Copyright information.

  

This screenshot shows the AWS S3 object details for "developer.txt". The main panel shows the object overview with the S3 URI. An inset browser window displays the contents of the file, which is "Hello World!". The bottom of the page includes standard AWS navigation links like Feedback, Language, and Copyright information.

## ■ cloudWatch-metric

The screenshot shows the AWS CloudWatch Metrics console. The left sidebar is collapsed, and the main area shows the Metrics section. A graph titled "Untitled graph" is displayed, showing a single data series from 10:00 to 12:45. Below the graph, there is a search bar and a grid of cards representing different metric categories: Billing (3), Config (214), Lambda (16), Logs (10), AWS/SecretsManager (1), States (8), and Usage (182). The bottom of the page includes standard AWS navigation links like Feedback, Language, and Copyright information.

- Security Groups if this required then in the question we need to correct it in task 4 the assignment

After validating the CloudWatch access granted to the role, navigate to the EC2 service and navigate to Security Groups. Within the submission template, under Steps 3 & 4 > Submission 3 provide a screenshot of successfully viewing a CloudWatch metric **Security Groups**.

The screenshot shows the AWS EC2 console with the URL `us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#SecurityGroups:`. The left sidebar is collapsed. The main area displays the 'Security Groups (1/1) Info' table. One row is present, representing the 'default' security group. The table columns include Name, Security group ID, Security group name, VPC ID, Description, Owner, Inbound rules count, and Outbound rules count. The 'default' entry has a security group ID of `sg-0a818852a0aaad825`, a VPC ID of `vpc-018bbecbcf8ea01b3`, and is owned by user `706648619117`. It contains 1 inbound rule and 1 outbound rule.

## ■ s3 objects tags

```
> aws s3api get-object-tagging --bucket legacy-developer-bucket-706648619117 --key developer.txt --output json | jq
{
  "TagSet": [
    {
      "Key": "Role",
      "Value": "developer"
    }
  ]
}
> aws s3api get-object-tagging --bucket legacy-developer-bucket-706648619117 --key analyst.txt --output json | jq
{
  "TagSet": [
    {
      "Key": "Role",
      "Value": "analyst"
    }
  ]
}
> aws s3api get-object-tagging --bucket analytics-report-bucket-706648619117 --key non_obfuscated.txt --output json | jq
{
  "TagSet": [
    {
      "Key": "Stage",
      "Value": "NonObfuscatedReport"
    }
  ]
}
> aws s3api get-object-tagging --bucket analytics-report-bucket-706648619117 --key obfuscated.txt --output json | jq
{
  "TagSet": [
    {
      "Key": "Stage",
      "Value": "ObfuscatedReportReady"
    }
  ]
}
4 > ↵ ~
```

## ■ Billing Console

The screenshot shows the AWS Billing Dashboard. On the left, a sidebar lists various billing-related services. The main area displays the AWS Summary, showing current month's total forecast (USD 0.00), current MTD balance (USD 0.00), and prior month's same period trend (USD 0.00, -0.0%). It also shows the total number of active services (1), active AWS accounts (1), and active AWS Regions (4). Below this, the Highest cost section highlights CloudWatch with a 0.0% trend compared to prior month, and a Current MTD balance of USD 0.00. A link to 'View your bill' is provided. At the bottom, a chart titled 'Cost trend by top five services' shows data over the last 3 months.

- Steps 5 & 6 >

- Submission 4

## ■ Lambda Code

```
import os
import json
import boto3
import datetime
from urllib.parse import unquote

RESTRICTED_RESOURCES = ["arn:aws:s3:::super-secret-bucket"]
ALERTING_ENABLED = False

def handler(event, context):
    print(event)
    invoking_event = json.loads(event["invokingEvent"])
    resource_type = invoking_event["configurationItem"]
    ["resourceType"]
    resource_id = invoking_event["configurationItem"]
    ["resourceId"]
    resource_arn = invoking_event["configurationItem"]["ARN"]
    restricted_resources_enabled = []

    if resource_type == "AWS::IAM::Policy":
        configuration = invoking_event.get("configurationItem",
        {}).get("configuration")
        if configuration:
            policy_version_list =
            configuration.get("policyVersionList", [])
            default_version = False
            for version in policy_version_list:
                if version.get("isDefaultVersion", False):
                    default_version = version
            if default_version:
                policy =
```

```

        json.loads(unquote(default_version["document"]))
            if type(policy["Statement"]) is list:
                for statement in policy["Statement"]:
                    if any(resource in RESTRICTED_RESOURCES for
resource in statement.get("Resource", [])):
                        client = boto3.client("config")
                        client.put_evaluations(
                            Evaluations=[
                                {
                                    'ComplianceResourceType': resource_type,
                                    'ComplianceResourceId': resource_id,
                                    'ComplianceType': 'NON_COMPLIANT',
                                    'Annotation': f'The policy has
a restricted resource listed',
                                    'OrderingTimestamp':
datetime.datetime.now()
                                },
                            ],
                            ResultToken=event["resultToken"]
                        )
            restricted_resources_enabled.append(resource_arn)
            if ALERTING_ENABLED and restricted_resources_enabled:
                print("ALERTING SNS")
                sns_client = boto3.client("sns")
                sns_client.publish(
                    TopicArn=os.environ["SNS_TOPIC"],
                    Message=f'The following policies have restricted resources
enabled {restricted_resources_enabled}'
                )

```

- Steps 5 & 6 >
  - Submission 5
    - bad-policy-that-breaks-enterprise-restrictions:

The screenshot shows the AWS Config console interface. The top navigation bar includes links for AWS Services, AWS Config, and a search bar. The main content area is titled "Resource Inventory" and displays a table of resources. The table has columns for "Resource identifier", "Type", and "Compliance". A single row is shown, labeled "bad-policy-that-breaks-enterprise-restrictions", which is identified as an "IAM Policy" and marked as "Noncompliant". The left sidebar contains navigation links for Dashboard, Conformance packs, Rules, Resources (with Aggregators expanded), and other sections like What's new, Documentation, Partners, FAQs, Pricing, and Share feedback.

Resource identifier	Type	Compliance
bad-policy-that-breaks-enterprise-restrictions	IAM Policy	Noncompliant

- Steps 7 >
  - Submission 6

■ organizational\_role\_diagram:

