S3 Bucket Access Checks Runbook

This runbook will guide you through the process of checking the access control settings for an S3 bucket using AWS CLI commands. It will help you verify permissions, policies, and other configurations to ensure proper access control to your S3 bucket.

Step 1: Install and Configure AWS CLI

- If you haven't already, install the AWS CLI on your local machine.
- Configure the AWS CLI with the necessary IAM credentials using `aws configure`.

Step 2: List All S3 Buckets Use the following command to list all S3 buckets in your AWS account:

bash

Copy code

```
aws s3 ls
```

Step 3: Check Bucket Policy To view the bucket policy for a specific bucket, run:

bash

Copy code

```
aws s3api get-bucket-policy --bucket YOUR_BUCKET_NAME
```

Ensure that the policy grants appropriate permissions to the intended users and roles.

Step 4: Check Bucket ACL (Access Control List) To view the ACL of the S3 bucket, run:

bash

Copy code

```
aws s3api get-bucket-acl --bucket YOUR_BUCKET_NAME
```

Ensure that the ACL settings allow the desired access for users and roles.

Step 5: Check Bucket Cross-Origin Resource Sharing (CORS) Configuration To check the CORS configuration of the bucket, run:

bash

Copy code

```
aws s3api get-bucket-cors --bucket YOUR_BUCKET_NAME
```

Ensure that the CORS settings are appropriately configured if your bucket is accessed by web applications from different origins.

Step 6: Check Bucket Default Encryption To check if default encryption is enabled for the bucket, run:

bash

Copy code

```
aws s3api get-bucket-encryption --bucket YOUR_BUCKET_NAME
```

Ensure that default encryption is enabled if required for sensitive data.

Step 7: Check Bucket Access Logging To verify if access logging is enabled for the bucket, run:

bash

Copy code

```
aws s3api get-bucket-logging --bucket YOUR_BUCKET_NAME
```

Ensure that access logging is appropriately configured for audit and monitoring purposes.

Step 8: Check Bucket Object Ownership To check the object ownership settings for the bucket, run:

bash

Copy code

```
aws s3api get-bucket-ownership-controls --bucket YOUR_BUCKET_NAME
```

Ensure that object ownership settings are configured as per your requirements.

Step 9: Check Bucket Public Access Block Configuration To verify the public access block configuration for the bucket, run:

bash

Copy code

```
aws s3api get-public-access-block --bucket YOUR_BUCKET_NAME
```

Ensure that public access is blocked for the bucket if it is not intended to be publicly accessible.

Step 10: Check Bucket Versioning To check if versioning is enabled for the bucket, run:

bash

Copy code

```
aws s3api get-bucket-versioning --bucket YOUR_BUCKET_NAME
```

Ensure that versioning is configured appropriately if required for data retention and protection.

Step 11: Check Bucket Replication (If Applicable) If the bucket has cross-region replication enabled, check its status by running:

bash

Copy code

```
aws s3api get-bucket-replication --bucket YOUR_BUCKET_NAME
```

Ensure that replication is correctly set up and monitored.

Step 12: Review IAM User and Role Policies Verify the IAM policies attached to users and roles that access the S3 bucket. You can use the AWS Management Console or AWS CLI to review IAM policies.

Step 13: Audit and Remediate Access Based on your analysis, ensure that proper access control is in place and make any necessary changes to policies, ACLs, or other configurations.