

CTAC PRIMER FOR AWS

How Control Testing Works

In summary, a Control Test is the programmatic collection and assessment of data from tested components to satisfy control objectives. One or more Control Tests run in a Test Suite on a scheduled interval. For each Control Test, a population is retrieved and sampled, then evidence is collected and assessed. Test outcomes are available in the Continuous Controls Control Testing Automation Center (CTAC) Power BI app. Evidence is located solely inside the customer evidence repository.

One or more Test Cases are executed as part of a logical group, called a Test Suite. Test Suites can be scheduled on manual, daily, weekly, monthly, or quarterly intervals. During this POC, your Test Suites will run daily, usually around noon CST. Test results are accessible in your CTAC Power BI Dashboard (more details below). For each Control Test included in a Test Suite during a Test Run, steps taken include:

1. Customer Bots collect population and evidence from the customer-managed systems. All data is stored within the customer's Evidence Repository.
2. Logical assessments are performed on the evidence to evaluate if the component passes or fails the control objective.



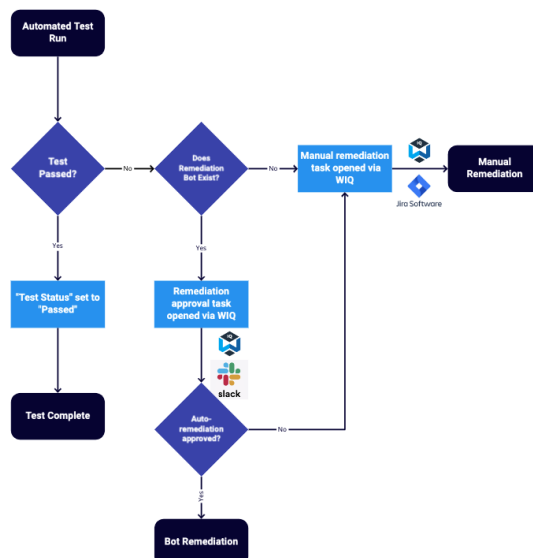
CTAC Control Testing



3. If failed, and a remediation bot exists, Workflow IQ sends an approval request to your team, and if approved, the bot then fixes the problem.
4. If failed, and a remediation bot exists, Workflow IQ sends an approval request to your team, and if not approved, a manual remediation task is opened for your team.
5. If failed, and no remediation bot exists, Workflow IQ opens a manual remediation task for your team.



CTAC Remediation Logic



How Bots Work

Continuous Controls uses customer-owned serverless computing and secure key management infrastructure for secure evidence collection and remediation tasks.

Bots

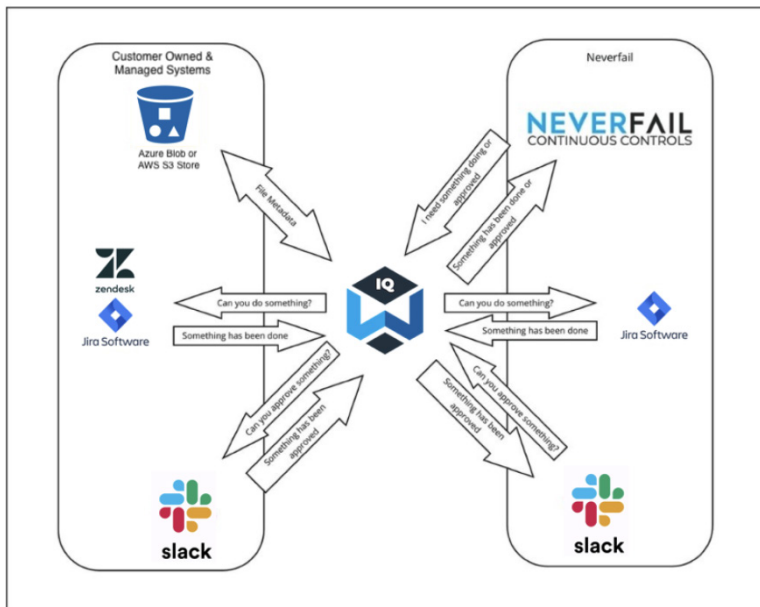
The Continuous Controls platform relies on customer “bots” to perform evidence collection and remediation tasks. Bots are customer-owned functions running in the AWS Lambda or Azure Functions serverless computing service. Each function is an independent unit of deployment, like a microservice, simply code, deployed in the cloud. A bot typically has a single function, such as collecting a particular evidence type, or ameliorating a particular failed condition. A single Control Test with remediation may use up to three different bots to operate, one for subjects, one for evidence, and another for remediation.

Secure Key Management

The Bots require secure API keys to operate. These keys are stored as “secrets” in a customer-owned secure key management service such as AWS Secrets Manager, or Azure Key Vault. When Continuous Controls platform needs evidence, it first calls on this service to retrieve the API key, then it uses this API key to securely call the customer bot. In this way, Neverfail operates in a fully secure, zero-trust architecture. The customer fully controls access to secrets using fine-grained permissions, and can revoke access at any time.

Workflow IQ

Workflow IQ (WIQ) securely connects customer task, approval, and storage systems to the CTAC platform. The customer can use a variety of supported services for approval, task, and storage features, such as JIRA, Slack, and S3 object storage, on a per-team basis. WIQ Tasks, Approval Requests, and Storage usage reporting and team management features are available in the WIQ web UI.



WIQ Approvals

During the POC, WIQ will be used for automated remediation approvals. When a test fails, if an automated remediation bot exists, CTAC will send an approval request to the team’s approval feature, such as a Slack channel. The request will provide details of the failed test and audited component, and enable users to approve or deny an automated remediation.

WIQ Tasks

During the POC, WIQ will also be used for manual remediation tasks. When a test fails, if no automated remediation bot exists, CTAC will send a manual remediation task to the team’s task feature, such as Jira.

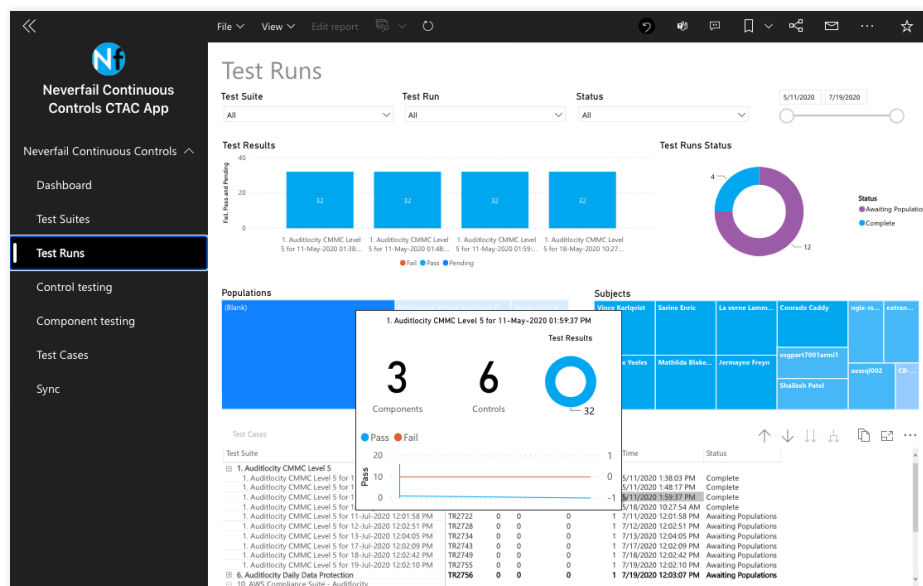
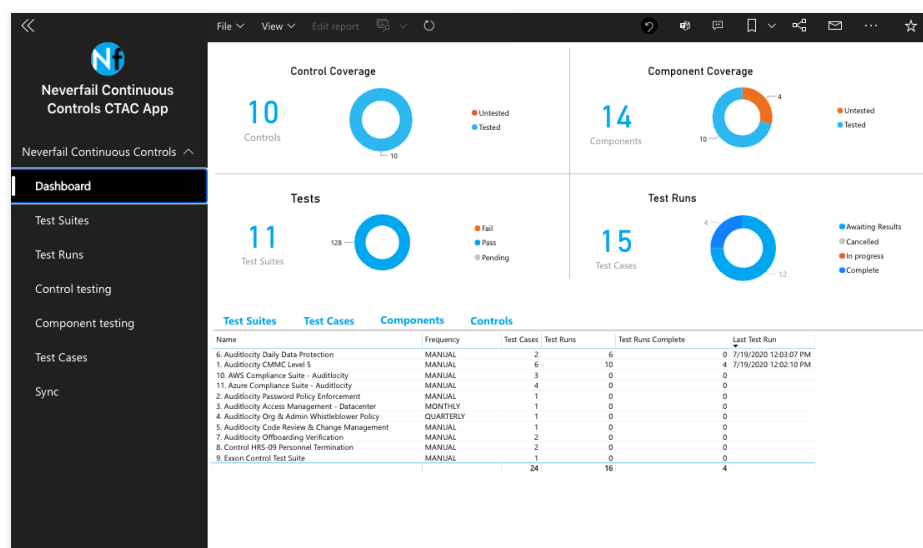
WIQ Storage

During the POC, WIQ will be used to store and serve customer data. For example, during test evidence collection, CTAC will call a customer's collection bot to collect the evidence from the customer's audited component. Inside the collection bot, WIQ writes the data inside the customer's evidence repository, which is simply a WIQ team's configured storage feature on an S3 bucket or Azure blob container. Though zero customer data is stored in CTAC, evidence metadata is available in CTAC to enable future requests for customer evidence via WIQ. During the assessment portion of a Control Test, CTAC uses the metadata to identify the location of the evidence, then calls WIQ to securely access it.

The Continuous Controls CTAC Power BI App

The CTAC Power BI App can be used to see reports with Control Testing details and outcomes over time. To access the app, please visit <https://app.powerbi.com> and open the app per the earlier deployment. Reports included:

- Test Suites
- Test Runs
- Control Testing
- Component Testing
- Test Cases
- Sync

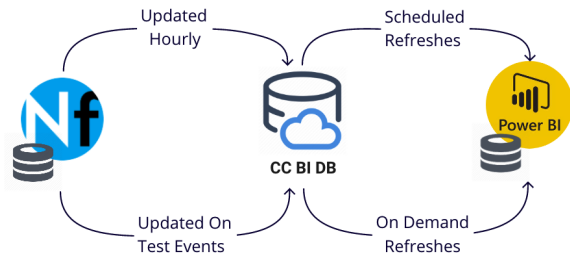


Data Synchronization

CTAC events such as Test Suite runs trigger data updates to the Neverfail CC BI database (CCBI DB). Updates are also performed hourly from CTAC to CCBI DB. The “Sync” report in the Power BI app will show the latest update time.

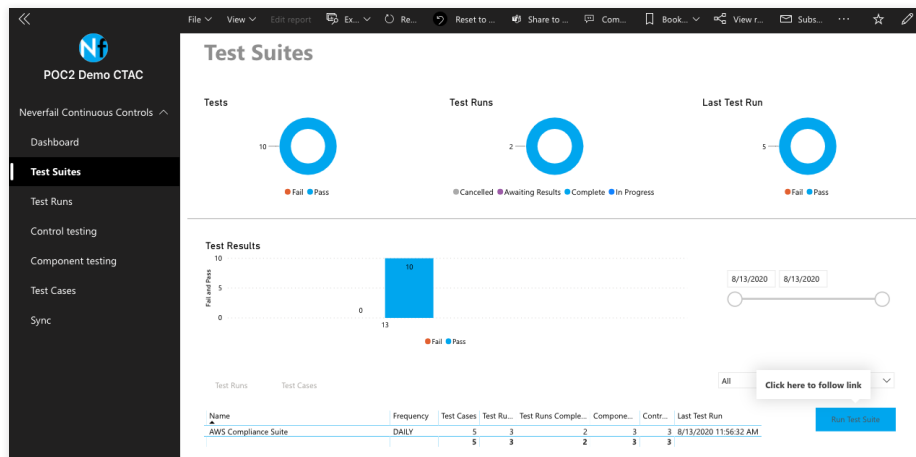
Power BI imports the data from the CCBI DB into its dataset on a scheduled frequency and on-demand. You might consider such a dataset a point-in-time copy. Because Power BI copies the data, you must refresh the dataset to fetch changes from the CCBI DB. Up to eight scheduled refreshes per day can be configured in PowerBI.

CTAC to Power BI Data Synchronization



Test Suite Runs

From the Test Suites report, you can launch new Test Suite Runs. When clicked, the Run Test Suite button will notify the CTAC platform to queue up a new Test Suite run. The actual execution of your Test Suite is determined by its place in the queue, and it may not run immediately, but generally should run within five minutes or less. Upon completion, updated data is sent to the CCBI DB, with a new sync time, and the PowerBI app dataset is ready to be refreshed. Currently, this feature allows up to five Test Suite Runs per 24-hour period, resetting the timer at 8am cst. These runs are in addition to the normal scheduled runs, which may be daily, weekly, monthly, or quarterly.

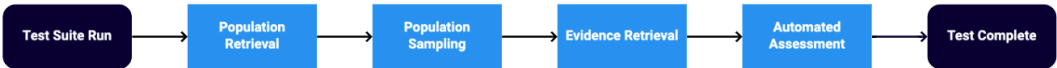
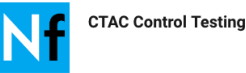


Control Test Walkthrough

As part of the POC, we will walk through a sample AWS Control Test from start to finish to learn how the collection bots interact with customer components to create population and evidence, how that evidence is assessed, and how to locate the evidence files in the customer Evidence Repository. For this Control Test walkthrough, we will use test “Production Relational Database Service (RDS) Databases Have Secure Configuration.” A common use of a DB instance in a VPC is to share data with an application server that is running in an EC2 instance in the same VPC. In this configuration, the RDS DB should not be publicly accessible, which is among the assessment criteria for this Control Test.

Control Test Walkthrough Goals

- Understand population and evidence retrieval
- Understand automated assessment logic
- Locate evidence in the evidence repository, including the Evidence Chain of Custody

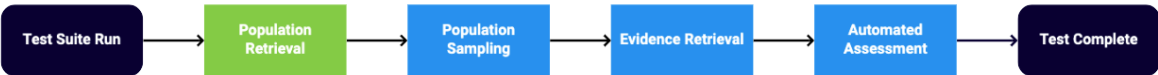


Control Test Details

Description	Production RDS Databases Have Secure Configuration
Tested Component	Production RDS Databases - US Regions
Subject - Population Type	DBaaS Instance - DBaaS Instance
Population Producer	Production RDS Databases - US Regions
Assessment Evidence Type	DBaaS Instance Security Configuration
Evidence Producer	Production RDS Databases - US Regions
Acceptance Criteria	Several criteria are assessed: backupRetentionPeriodDays (int), API Property: DBInstances.BackupRetentionPeriod, Pass condition: > 0 secondaryAvailabilityZone (string), API property: DBInstances.SecondaryAvailabilityZone, Pass condition: Not Null assetStorageEncrypted (boolean), API property: DBInstances.StorageEncrypted, Pass condition: True assetPublicAccess (boolean), API property: DBInstances.PubliclyAccessible, Pass condition: False networkTcpPort (string), API property: DBInstances.Endpoint.Port, Pass condition: not required/assessed

Population Retrieval

The population for this test is the set of RDS DBaaS instances tagged with the “environment”:“nfcc-production” tag. The customer collection bot uses APIs to retrieve the matching instances from AWS RDS. Once the population data is collected, WIQ will store it in the evidence repository as JSON documents.



```
{
  "dbName": "sitest-db-1",
  "dbEngine": "oracle-se1",
  "dbEngineVersion": "11.2.0.4.v24",
  "dbEndpoint": "sitest-db-1.celahfvvcgyll.us-east-2.rds.amazonaws.com",
  "dbInstanceArn": "arn:aws:rds:us-east-2:876393867294:db:sitest-db-1",
  "awsRegionId": "us-east-2",
  "awsRegionName": "US East (Ohio)",
  "environment": "nfcc-production"
}
```

Example RDS Population JSON Document

Population Sampling

Test subjects are sampled from a population before a Control Test. The sampling rate is adjustable. The POC defaults to 100% sampling, meaning the entire population is subject to control testing.



Evidence Retrieval

Because this Control Test is assessing several security configuration settings, the required evidence consists of a structured list of those settings for that particular DB. The next step is to retrieve this evidence for each subject, using another collection bot. Again, once the evidence data is collected, WIQ will store it in the evidence repository as JSON documents.



```

{
  "assetId": "sitest-db-1.celahfvcgyll.us-east-2.rds.amazonaws.com",
  "assetType": "rdsInstance",
  "assetName": "sitest-db-1",
  "backupRetentionPeriodDays": 0,
  "assetStorageEncrypted": true,
  "assetPublicAccess": true,
  "networkTcpPort": 1521,
  "awsRegionId": "us-east-2"
}
  
```

Example DBaaS Instance Security Configuration Evidence JSON Document

Automated Assessment

For each Control Test, a logical assessment is performed on the collected evidence to determine if the required conditions are satisfied (pass) or not (fail). For this assessment, we are checking the DBaaS instance's public accessibility, backup retention, and storage encryption settings. You will notice that the evidence includes the network TCP port of the DBaaS instance as an informational datapoint, however it is not assessed. If your organization requires certain commonly-exploited ports were banned from use, such as TCP 1433, we would implement this evidence type in a different Control Test, one that evaluates that port for policy violations. For every Control Test, the assessment logic required is described in "Gherkin," a business-readable, ordinary language parser. The "Gherkin" for this Control Test is shown below:

Scenario: Check if RDS DBs are secured
Given a DBaaS instance as subject
And a security config policy as evidence
When I get security config values
Then value of backupRetentionPeriodDays should be greater than 0
And value of assetStorageEncrypted should be true
And value of assetPublicAccess should be false

Example of Gherkin



Evidence Review

With the assessment completed, the Control Test is now done and the Evidence Chain of Custody is being generated. For each piece of evidence, CTAC automatically synthesizes its collection logs into an Evidence Chain of Custody, a process which takes up to seven minutes to complete. The Evidence Chain of Custody is itself considered another piece of evidence and is also stored in the Evidence Repository. To access the Evidence Repository directly, use the AWS S3 portal to navigate to the S3 bucket, as configured in the WIQ storage team feature. From here, you will see a list of objects, each of these being either a piece of evidence or an Evidence Chain of Custody. Feel free to select, then **Open** any of them. Generally, the ones that are of a larger size will be the Evidence Chain of Custody records.

Manual Remediation Walkthrough

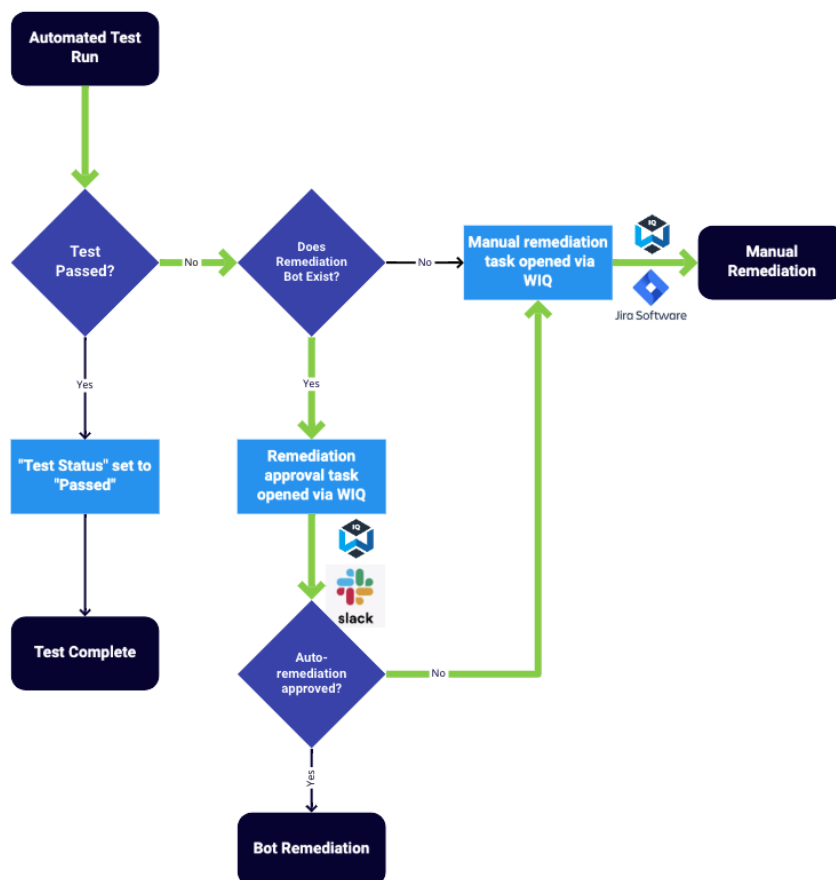
We will now walk through a sample manual remediation task to learn how to manually remediate a failed test condition. For this manual remediation sample review, we will continue to use the test from the last section, "Production Relational Database Service (RDS) Databases Have Secure Configuration." Manual remediation tasks are the default outcome for failed tests where no remediation bot exists for that particular failed condition. In this walkthrough, because we do have a remediation bot, we will have to reject the automated remediation WIQ Approval to get us to a manual remediation task.

Manual Remediation Walkthrough Goals

- Understand how changes to the infrastructure alter control test outcomes
- Understand how to perform a manual remediation WIQ Task



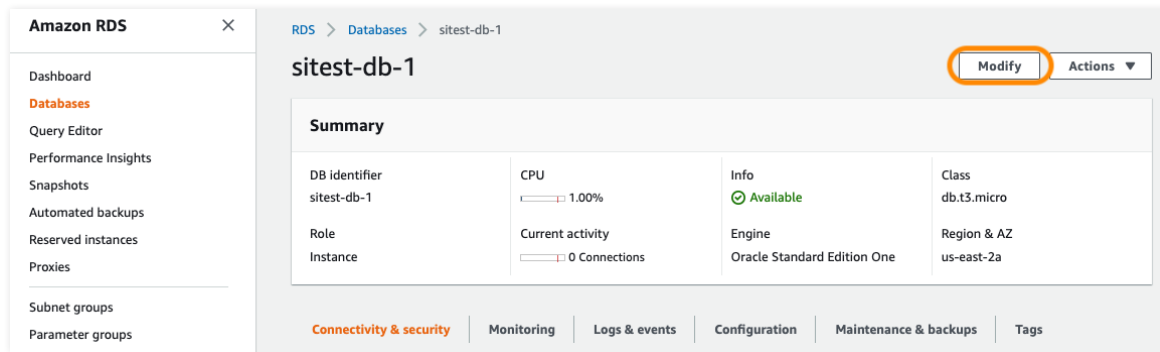
CTAC Remediation Logic



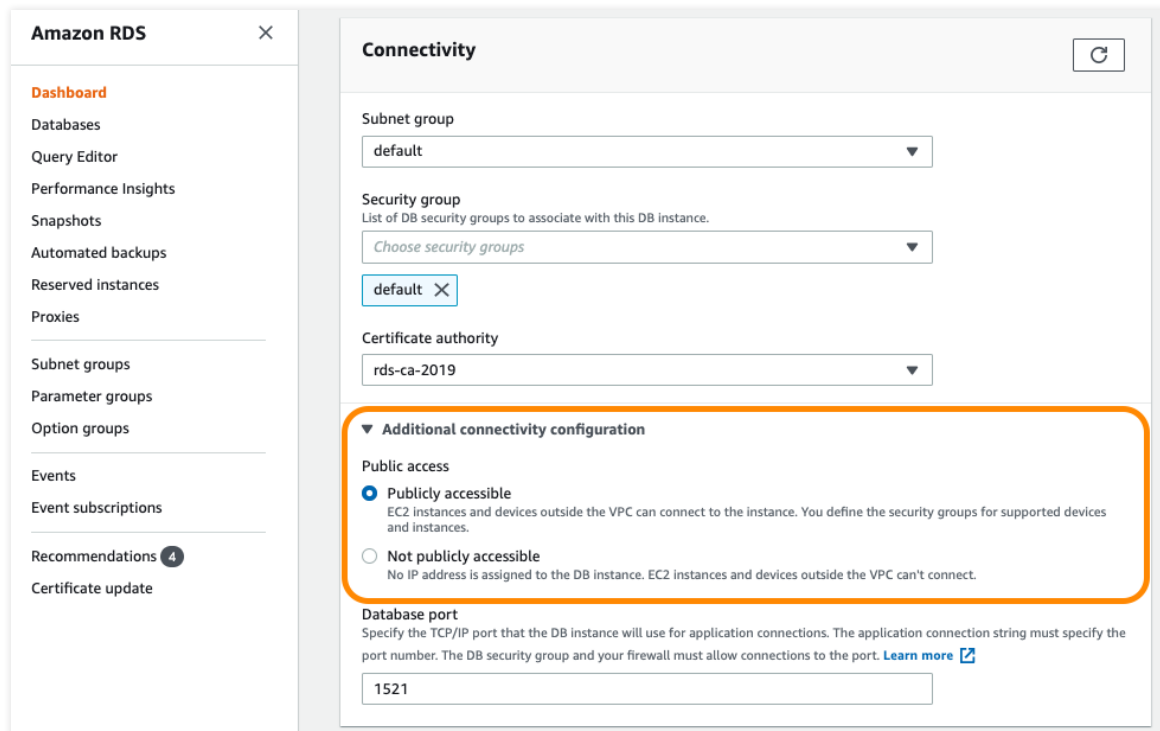
Preparing for Manual Remediation

In order to exhibit a manual remediation process using WIQ, we will need to set failing conditions for the assessment, by setting public accessibility to “true” for our RDS DBaaS instance.

1. From the Amazon RDS console, navigate to the database list by clicking **Databases** on the left.
2. Click on the database that has a label similar to “customer-name-db-1.”
3. Click the Modify button on the upper-right of the window.



4. Scroll down to the “Connectivity” section, and look for the “Public Access” settings, then set the option to **Publicly accessible**. You may need to expand a section called “Additional connectivity configuration” to access this setting.



5. Scroll down further and click **Continue**.

6. On the next screen, set Scheduling of modifications to **Immediately** and click **Modify DB instance**.

RDS > Databases > Modify DB instance: sitest-db-1

Modify DB instance: sitest-db-1

Summary of modifications

You are about to submit the following modifications. Only values that will change are displayed. Carefully verify your changes and click Modify DB Instance.

Attribute	Current value	New value
Public accessibility	No	Yes

Scheduling of modifications


When to apply modifications

☐ During the next scheduled maintenance window

Current maintenance window: tue:05:00-tue:05:30

☒ Immediately

This upgrade and any pending modifications will be asynchronously applied as soon as possible, regardless of the maintenance window setting for this database instance.

 Potential unexpected downtime

If you choose to apply changes immediately, please note that any changes in the pending modifications queue are also applied. If any of the pending modifications require downtime, choosing this option can cause unexpected downtime.

Cancel

Back

Modify DB instance

7. Because AWS RDS takes some time to enact the changes, please wait 1-2 minutes and verify that the setting has changed by refreshing the database view until you see Public accessibility setting set to “Yes.”

Amazon RDS

Dashboard

Databases

Query Editor

Performance Insights

Snapshots

Automated backups

Reserved Instances

Proxies

Subnet groups

Parameter groups

Option groups

Events

Event subscriptions

Recommendations 2

Certificate update

Summary

DB Identifier	CPU	Info	Class
aws24poc-db-1	<div>1.00%</div>	Modifying	db.t3.micro
Role	Current activity	Engine	Region & AZ
Instance	<div>0 Connections</div>	Oracle Standard Edition One	us-west-1a

Connectivity & security

Monitoring

Logs & events

Configuration

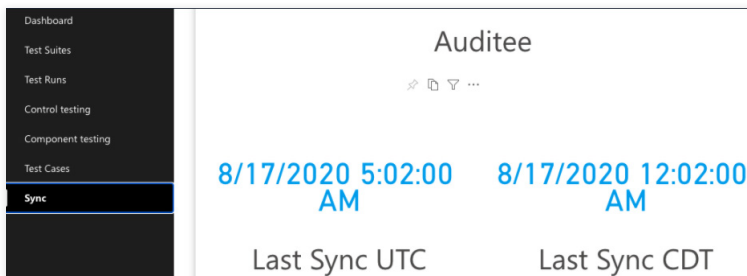
Maintenance & backups

Tags

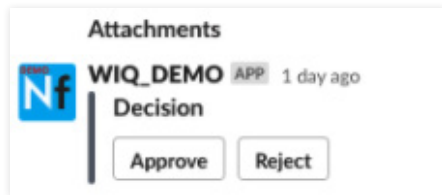
Connectivity & security

Endpoint & port	Networking	Security
Endpoint	Availability zone	VPC security groups
aws24poc-db-1.cvhsvfjbvrhd.us-west-1.rds.amazonaws.com	us-west-1a	default (sg-961091e3) (active)
Port	VPC	Public accessibility
1521	vpc-2f36c849	Yes
	Subnet group	Certificate authority
	default	rds-ca-2019
	Subnets	Certificate authority date
	subnet-ec379e8a	Aug 22nd, 2024
	subnet-f033f6aa	

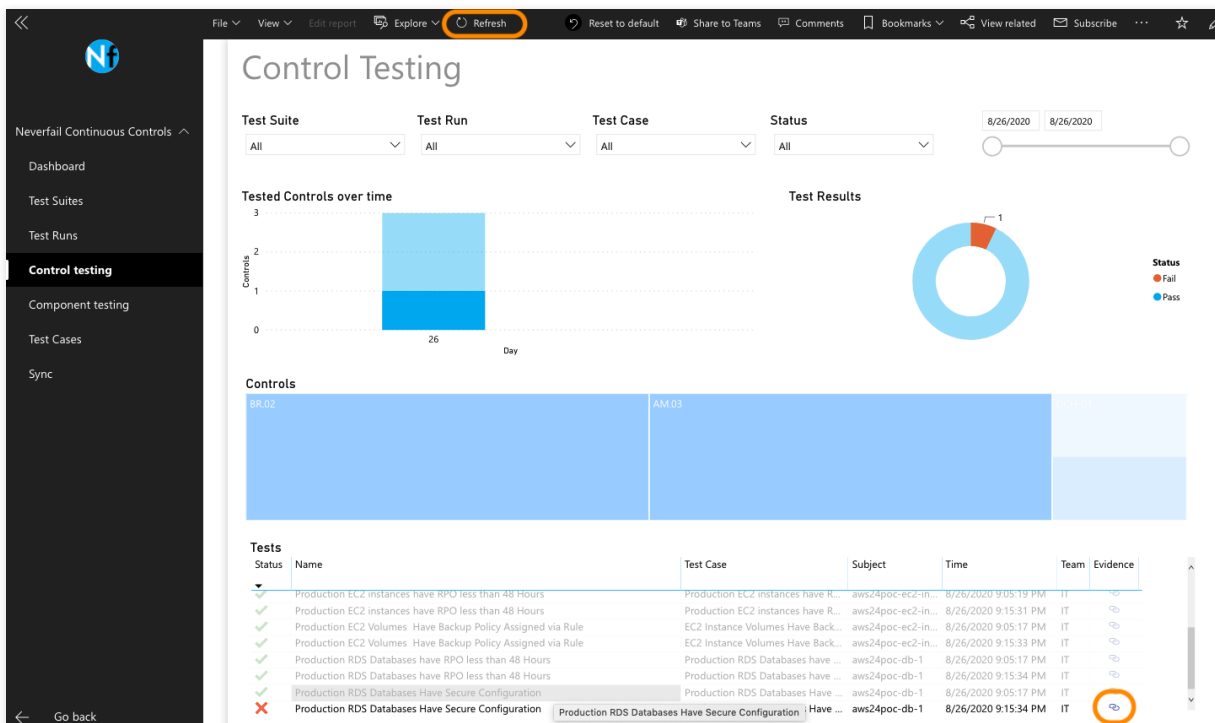
8. Now we trigger another Test Run so we can see the test in a failed assessment state. Go to the Power BI app (<http://app.powerbi.com/>), navigate to the Test Suite view, then run the AWS Compliance Test Suite. Remember, the Run Test Suite button will notify the CTAC platform to queue up a new Test Suite run. The actual execution of your Test Suite is determined by its place in the queue, and it may not run immediately, but generally should run within five minutes or less.
9. Wait five minutes for the test to rerun and update the CC BI DB. Refresh your dataset in your Power BI app to pull the latest copy of data. Please visit Appendix A at the end of this document to review your dataset refresh methods.
10. Check the Sync report to see when the last data sync occurred between the testing platform and the CC BI DB. It should reflect the most recent run time. If it doesn't, refresh the dataset again.



11. Because a remediation bot exists to fix this condition, a WIQ approval will be opened in your configured WIQ Approval system. For the purposes of this manual remediation walkthrough, we need you to Reject this request so that WIQ opens a manual remediation task for your team. We will cover WIQ Approvals in more detail in the next section, Automated Remediation Walkthrough.



12. Now inside the app, visit Control Testing, and you should see a failed test. If you do not see this failed test, please try clicking the **Refresh** button above the dashboard.



- Click on the link icon under the Evidence column for the failed test to see the JSON document evidence. As you can see, `assetPublicAccess` is set to `true`, which fails the assessment.

```
{
  "assetId": "sitest-db-1.celafhvcgyl.us-east-2.rds.amazonaws.com",
  "assetType": "rdsInstance",
  "assetName": "sitest-db-1",
  "backupRetentionPeriodDays": 0,
  "assetStorageEncrypted": true,
  "assetPublicAccess": true,
  "networkTcpPort": 1521,
  "awsRegionId": "us-east-2",
  "awsRegionName": "US East (Ohio)"
}
```

Example Failing DBaaS Instance Security Configuration Evidence JSON Document

Manual Remediation Using the WIQ Task

At this point you should now have a new remediation task in your configured WIQ task system. To remediate this test condition, you need to set that RDS DBaaS instance to not be publicly accessible, then close the task.

- Visit your configured Task system to see your new remediation task.
- Follow the instructions from the last section, steps 1-4, but instead of setting Public Access to "Publicly accessible," set it to "Not publicly accessible."
- Scroll down further and click **Continue**.
- On the next screen, set Scheduling of modifications to **Immediately** and click **Modify DB instance**.

RDS > Databases > Modify DB instance: sitest-db-1

Modify DB instance: sitest-db-1

Summary of modifications

You are about to submit the following modifications. Only values that will change are displayed. Carefully verify your changes and click Modify DB Instance.


Attribute	Current value	New value
Public accessibility	Yes	No

Scheduling of modifications

When to apply modifications

☐ During the next scheduled maintenance window
 Current maintenance window: tue:05:00-tue:05:30

☒ Immediately
 This upgrade and any pending modifications will be asynchronously applied as soon as possible, regardless of the maintenance window setting for this database instance.



Potential unexpected downtime

If you choose to apply changes immediately, please note that any changes in the pending modifications queue are also applied. If any of the pending modifications require downtime, choosing this option can cause unexpected downtime.

Cancel
Back
Modify DB instance

- Because AWS RDS takes some time to enact the changes, please wait 1-2 minutes and verify that the setting has changed by refreshing the database view until you see Public accessibility setting set to "No."
- Complete the WIQ Task in your task system.
- Now we trigger another Test Run so we can see the test in a passed assessment state. Go to the Power BI app (<http://app.powerbi.com/>), navigate to the Test Suite view, then run the AWS Compliance Test Suite.
- Wait five minutes for the test to run and update the CC BI DB. Refresh your dataset in your Power BI app to pull the latest copy of data. You can refresh as often as needed.
- Now inside the app, visit Control Testing, and you should see the passed test. If you do not see this passed test, please try clicking the **Refresh** button above the dashboard.
- On the Control Testing report, feel free to click on the link icon under the Evidence column for the passed test to see the JSON document evidence. As you can see, assetPublicAccess is set to false, which passes the assessment.

```
{
  "assetId": "sitestest-db-1.celahfvcgyl.us-east-2.rds.amazonaws.com",
  "assetType": "rdsInstance",
  "assetName": "sitestest-db-1",
  "backupRetentionPeriodDays": 0,
  "assetStorageEncrypted": true,
  "assetPublicAccess": false,
  "networkTcpPort": 1521,
  "awsRegionId": "us-east-2",
  "awsRegionName": "US East (Ohio)"
}
```

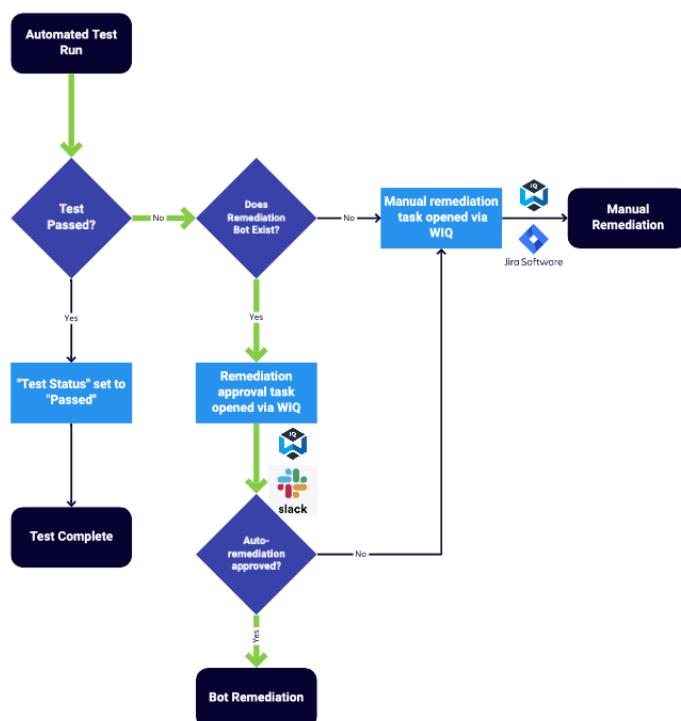
Example Passing DBaaS Instance Security Configuration Evidence JSON Document

Automated Remediation Walkthrough

We will now walk through another sample AWS Control Test to demonstrate how automated remediation works. For this automated remediation sample, we will use test: "Public Access Blocked on S3 Cloud Storage."



CTAC Remediation Logic



Automated Remediation Walkthrough Goals

- Break the conditions of the assessment on a Control Test to trigger an automated remediation
- Understand how automated remediation via WIQ operates

Control Test Details

Description	Public Access Blocked on S3 Cloud Storage
Tested Component	S3 Production Object Storage
Subject - Population Type	Object Store - Production Object Store Bucket Population
Population Producer	S3 Production Object Storage
Assessment Evidence Type	AWS S3 Security Policy
Evidence Producer	S3 Production Object Storage
Acceptance Criteria	<p>Zero public access to the resource (bucket).</p> <p>Ensure the following are enabled for a given bucket:</p> <p>Block public access to buckets and objects granted through new access control lists (ACLs)</p> <p>Block public access to buckets and objects granted through any access control lists (ACLs)</p> <p>Block public access to buckets and objects granted through new public bucket or access point policies</p> <p>Block public and cross-account access to buckets and objects through any public bucket or access point policies</p> <p>PublicAccessBlockConfiguration: { BlockPublicAcls: true, IgnorePublicAcls: true, BlockPublicPolicy: true, RestrictPublicBuckets: true }</p>

Gherkin	<p>Scenario: Check if amazon buckets are publicly exposed</p> <p>Given an amazon bucket as subject from a list of buckets</p> <p>And a public policy for selected bucket as evidence</p> <p>When I get the values of blockPublicPolicy, blockPublicAcls, ignorePublicAcls, restrictPublicBuckets</p> <p>Then values should be set to true</p>
Evaluation Type	Inspection
Test Type	Automated

Preparing for Automated Remediation

In order to exhibit an automated remediation process using WIQ, we need to enable public access to a production S3 object storage bucket to cause the next assessment to fail.

1. From the AWS console, select Storage -> **S3** (or search for “S3”) to access the Amazon S3 console.
2. Review the bucket list and click on the one with label “CUSTOMER_NAME-neverfail-s3-production-object-storage-1.” This is an S3 bucket with a special tag applied of “environment”:“nfcc-production,” which simulates tag application in the real-world.
3. On the bucket detail view, click the **Permissions** tab to view the access settings.
4. Under the **Block public access** section, click the **Edit** button on the far right-hand side.

5. Uncheck **Block all public access** checkbox, then click **Save**.

audjul27-neverfail-s3-production-object-storage-1

Overview Properties Permissions Management Access points

Block public access Access Control List Bucket Policy CORS configuration

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☐ **Block all public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☐ **Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☐ **Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.

☐ **Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☐ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Cancel Save

6. If you get a confirmation window, follow the instructions.

Edit block public access (bucket settings) ✕

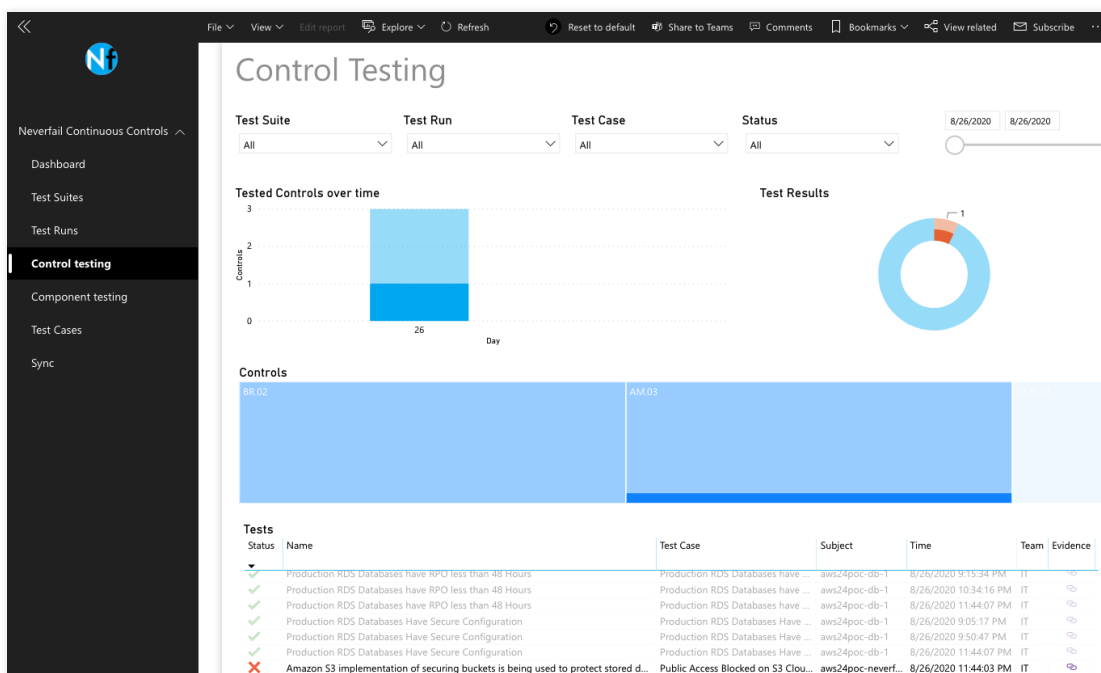
Updating the block public access (bucket settings) will affect this bucket and all objects within. This may result in some objects becoming public.

To confirm the settings, type *confirm* in the field.

confirm

Cancel Confirm

7. Now we trigger another Test Run so we can see the test in a failed assessment state. Go to the Power BI app (<http://app.powerbi.com/>), navigate to the Test Suite view, then run the AWS Compliance Test Suite.
8. Wait five minutes for the test to run and update the CC BI DB. Refresh your dataset in your Power BI app to pull the latest copy of data. You can refresh as often as needed. If you do not see updated data, try clicking the **Refresh** button above the dashboard.



- On the Control Testing report, feel free to click on the link icon under the Evidence column for the passed test to see the JSON document evidence. The block "publicAcls" are set to false, which fails the assessment.

Automated Remediation via a WIQ Approval Request

CTAC will detect if the remediation bot exists for the particular failed condition. If the remediation bot exists, it will send a WIQ Approval Request to the customer team's approval system before taking any action.



WIQ_DEMO APP 1 day ago

Description

There is an automated testing remediation available for a failed test '51043':

Test Run:

10. AWS Compliance Suite - Auditlocity for
25-Aug-2020 02:00:09 PM

Test Case:

Amazon S3 implementation of securing buckets is being used to protect stored data.

Test Subject JSON:

```
{"bucketName":"bucket-auditlocity-0", "url":"bucket-auditlocity-0.s3.amazonaws.com/"}
```

Tested Component:

S3 Production Object Storage

Test Failure Message:

Values of blockPublicPolicy, blockPuclicAcls, ignorePublicAcls, restrictPublicBuckets should be true

Applicable Exception Data:

```
{"bucketName":"bucket-auditlocity-0","blockPublicPolicy":false,"blockPuclicAcls":false,"ignorePublicAcls":false,"restrictPublicBuckets":false}
```

Please approve or reject the automated remediation of this exception:

[See less](#)

- Navigate to the configured approval system and review the new approval request.
- Click **Approve**.
- When prompted, input time spent in minutes.
- The remediation bot will be called and the configuration ameliorated.
- Now we trigger another Test Run so we can see the test in a passed assessment state. Go to the Power BI app (<http://app.powerbi.com/>), navigate to the Test Suite view, then run the AWS Compliance Test Suite.
- Wait five minutes for the test to rerun and update the CC BI DB. Refresh your dataset in your Power BI app to pull the latest copy of data. You can refresh as often as needed.
- Now inside the app, visit Control Testing, and you should see the passed test. If you do not see this passed test, please try clicking the **Refresh** button above the dashboard.

Attachments



WIQ_DEMO APP 1 day ago

Decision

Approve

Reject

Evidence Review Walkthrough

Before proceeding, we recommend you have a JSON document formatter web browser extension to ensure the data files are legible. For Chrome, some options include [JSONView](#), [JSONFormatter](#), or [PrettyJSON](#) (though we do not recommend any particular extension).



1. From the AWS console, select Storage -> **S3** (or search for "S3") to access the Amazon S3 console.
2. Review the bucket list and locate one with the label "CUSTOMER_NAME-neverfail-s3-evidence-repository-1." This is your Evidence Repository.
3. Click on the bucket link, then click again on the folder within it.
4. From here, you will see a list of objects, each of these being either a piece of evidence or an Evidence Chain of Custody. Feel free to select, then **Open** any of them. Generally, the ones that are of a larger size will be the Evidence Chain of Custody records.

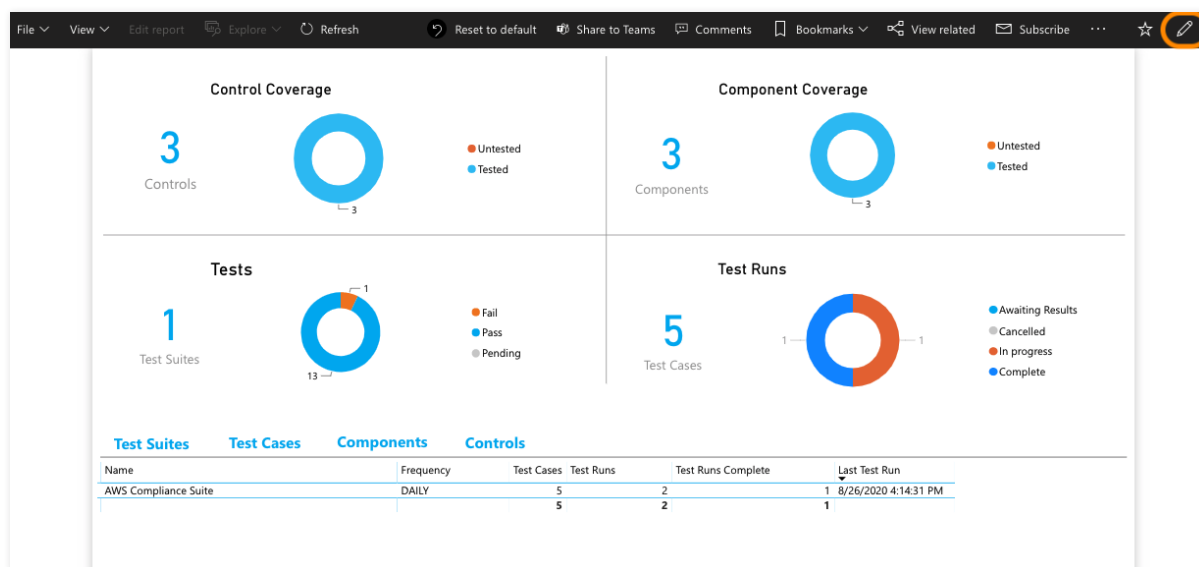
Appendix A

Scheduling Data Refreshes in Power BI

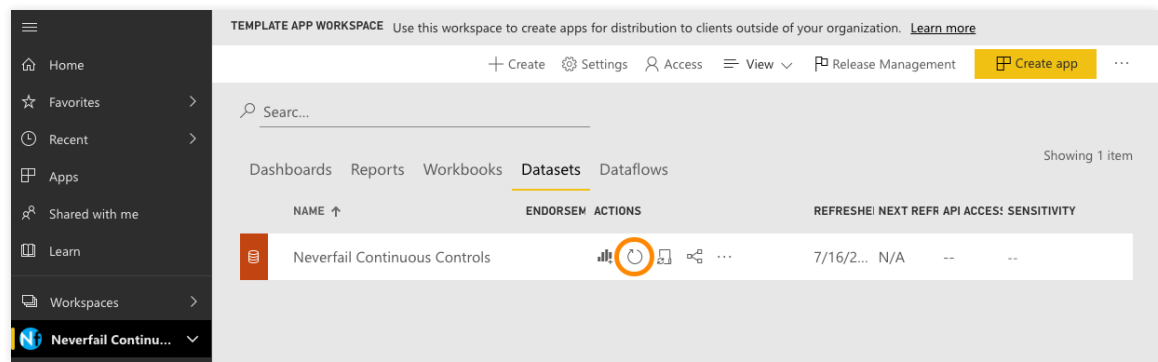
You have two options by which to refresh the data in your CTAC Power BI app, on-demand, or scheduled.

On-demand Data Refresh

1. In the app, click the **pencil icon** on the upper-right to edit settings.

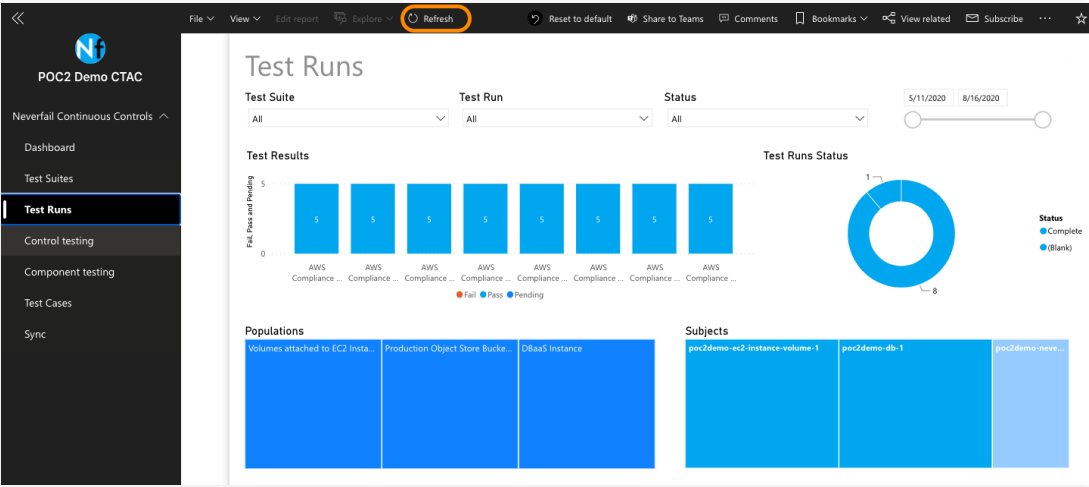


2. Click the **Datasets** label then click the Refresh icon, per screenshot below.



Still Not Updating?

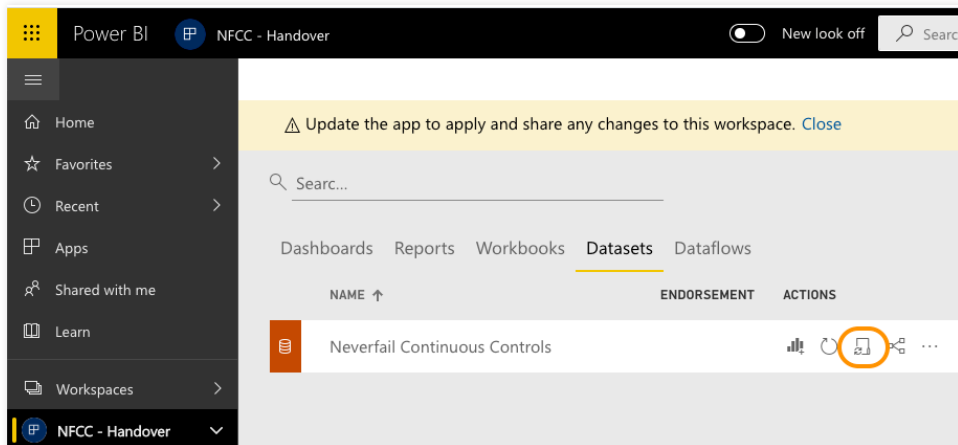
Please note that even after a dataset refresh, your app's report views may show outdated data. If this happens, please hit the refresh button on the report view, per screenshot below.



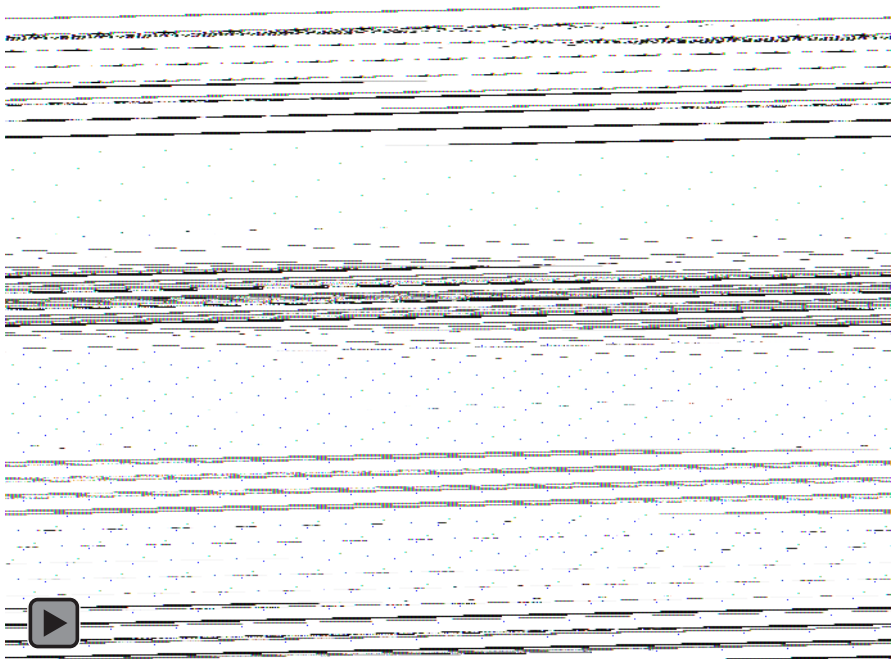
Scheduled Data Refresh

During your POC, you may want to schedule the refreshes to run automatically. Power BI allows for up to eight total data refreshes per day. If you want to schedule the refreshes, we recommend to set the refresh frequency to hourly during work hours, per image below.

1. Navigate to the **Workspaces** area using the left-hand menu.
2. Click on the Workspace for this app.
3. Click the **Datasets** label then click the Schedule Refresh icon, per screenshot below.



4. Expand and set the Scheduled refresh section to have up to eight refreshes. Consider setting them during normal work hours, at the bottom of the hour.
5. Click **Apply** to save.



► Gateway connection

► Data source credentials

► Parameters

4 Scheduled refresh

Keep your data up to date

☒ On

Refresh frequency

Time zone

Time

8	30	AM	X
9	30	AM	X
10	30	AM	X
11	30	AM	X
12	30	PM	X
1	30	PM	X
2	30	PM	X
3	30	PM	X

Reviewing Latest Sync Time

On the Sync report in the app, you will find the timestamp of the latest data update event from the CTAC platform to the CC BI server, from where your PowerBI app retrieves its copy of data.

Dashboard	Auditee	
Test Suites	✱ 📄 ▼ ...	
Test Runs		
Control testing		
Component testing		
Test Cases		
Sync	8/17/2020 5:02:00 AM	8/17/2020 12:02:00 AM
	Last Sync UTC	Last Sync CDT