Introducing the IBM Cloud Framework for Financial Services

This document will walk you through a demonstration of how to introduce the IBM Cloud Framework for Financial Services. This will enable you to explain how the FS controls as we sometimes refer to them can show how automated compliance can be proven from an FS Cloud architecture. The controls link into the Security and Compliance center FS Cloud Profile and can be scanned for validation. We also help show the mapping between the FS Controls and the cloud services used in the FS Cloud Reference architecture.

Goals for the Demo:

- Familiarize the audience with IBM Cloud Framework for Financial Services.
- Explain the Control Families, Control details and guidance from IBM and for the ISV and Ecosystem partner
- Demonstrate the mapping between the FS Controls and the Cloud services used in a an FS Cloud reference architecture.

Prerequisites:

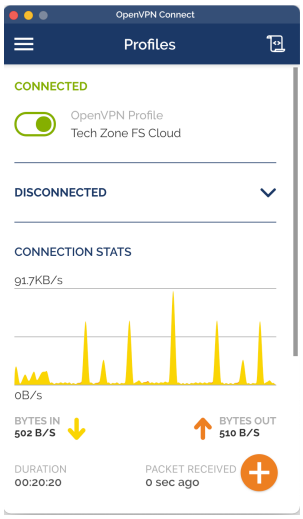
- If you have not already done so, request access to the FS Cloud demo environment at: https://techzone.ibm.com/collection/ibm-cloud-for-financial-services

- Download and install the OpenVPN client
  - Windows https://openvpn.net/community-downloads/
  - MacOS https://openvpn.net/client-connect-vpn-for-mac-os/
  - Linux https://openvpn.net/download-open-vpn/

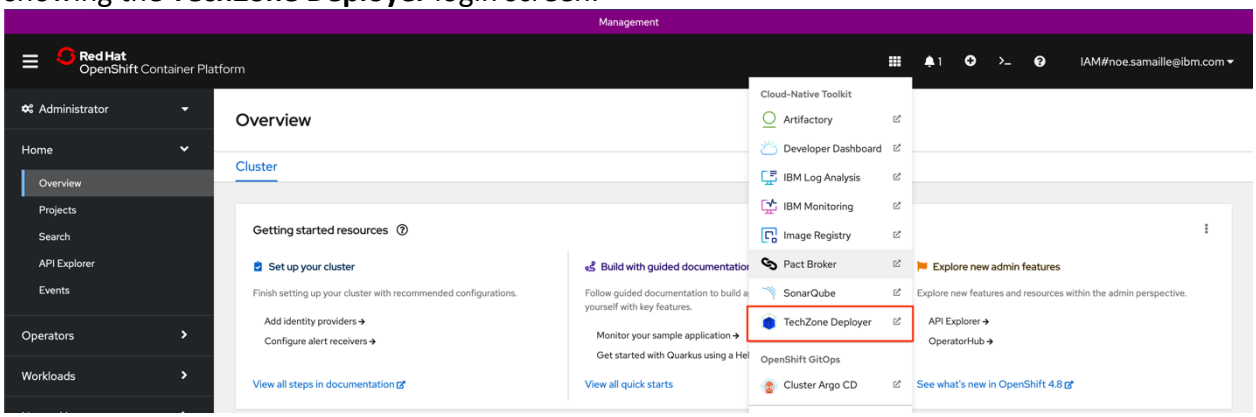
- Download the **techzone.ovpn** VPN certificate and add it to the OpenVPN client
  - Link https://techzone-iam-agent.eqtyaj6hk2k.eu-de.codeengine.appdomain.cloud/vpn/download

Steps:

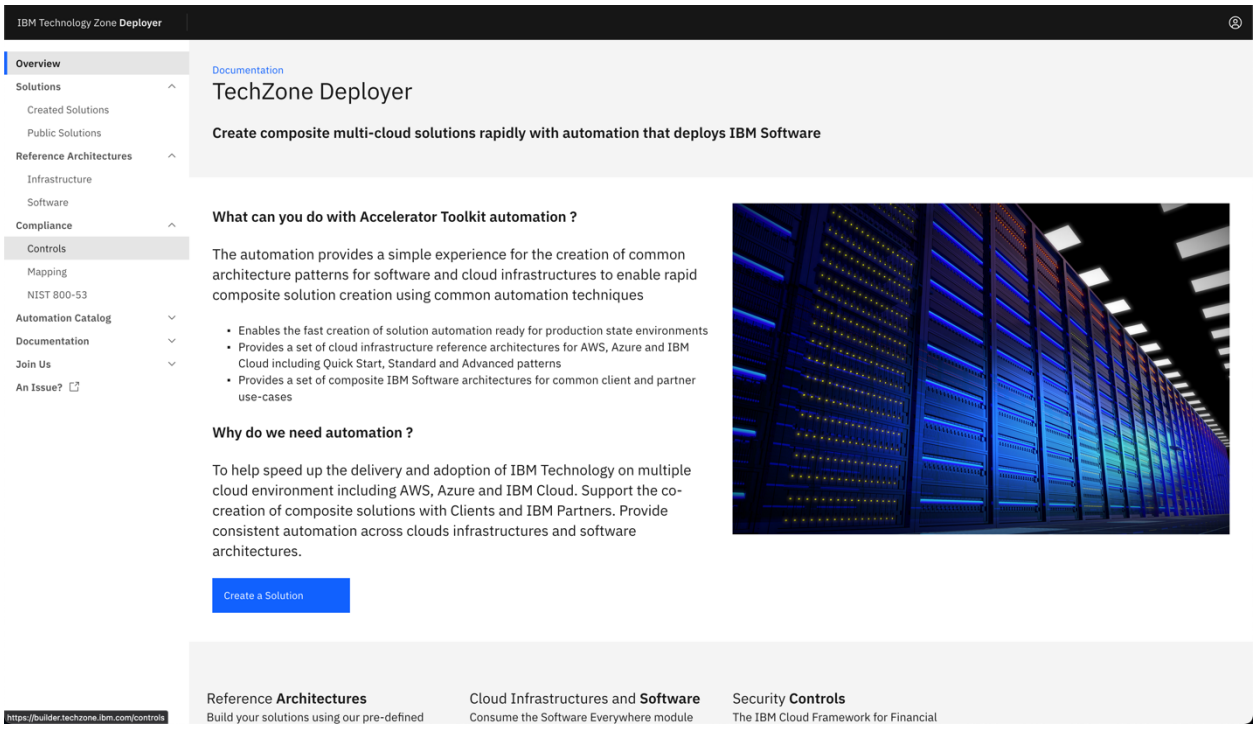
1. Connect the OpenVPN Client with the Tech Zone demo profile



2. Login to IBM Cloud https://cloud.ibm.com
3. For official documentation of the IBM Cloud for Financial Services controls framework, navigate to https://cloud.ibm.com/docs/framework-financial-services?topic=framework-financial-services-about
4. In this lab, we will use an accelerator tool created by the Ecosystem Engineering team to easily navigate and understand the controls framework.
5. Navigate to the Resource View https://cloud.ibm.com/resources
6. Expand the **Cluster** twisty and click on **management-cluster**
7. Click on **OpenShift Web Console** make sure you OpenVPN client is running and connected, you should see the **Management Cluster**
8. Click on the 9 Square menu and select **TechZone Deployer** you will the following screen showing the **TechZone Deployer** login screen.

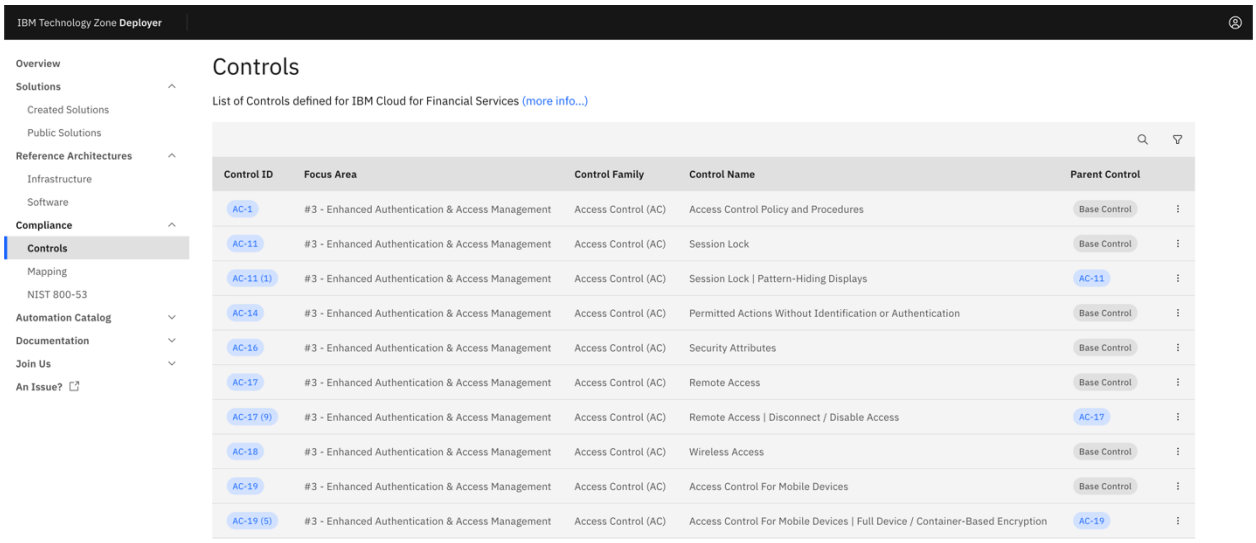


9. Click on the **Login** button click on the Profile icon top right and validate you are logged into the tool correctly.

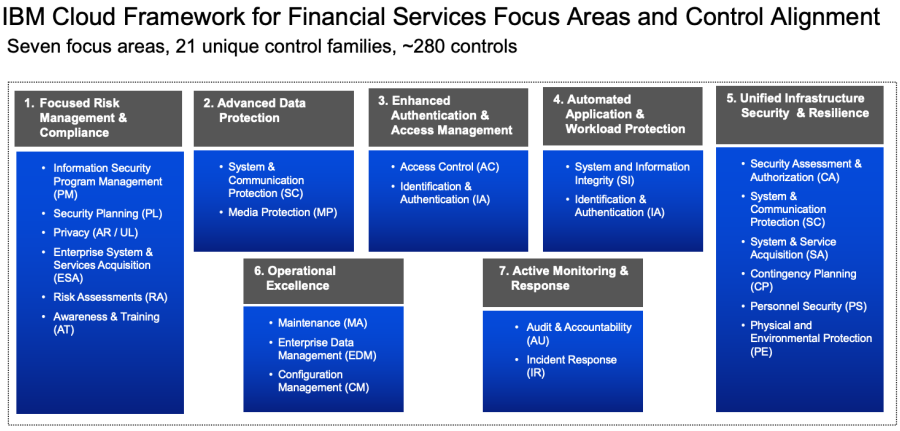


10. On the menu on the left select **Compliance -> Controls** this will display the list of controls.

11. Controls define the compliance requirements that a Risk team or Compliance officer will need the validate for a solution implemented on IBM Cloud.

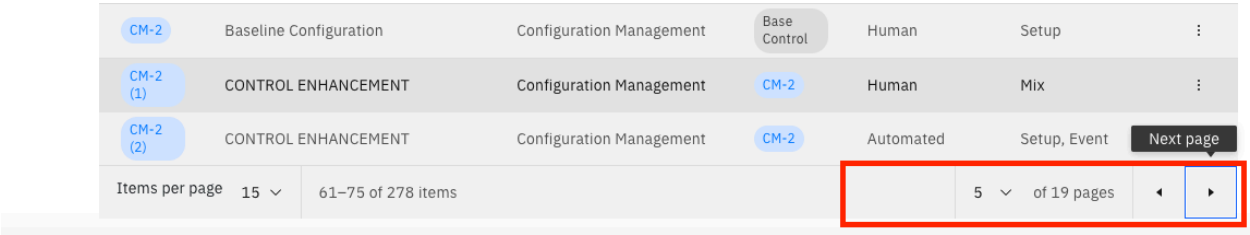


12. Scroll down the page and highlight there are **280** controls, and each control has a set of sub controls detailing nearly **600** controls that need to be validated.
13. Highlight that each control must be validated through Automation, SCC console scan or by humans or a mix of both.
14. Highlight those controls can be validated at project inception setup or continuously or at various time slots during the project year.

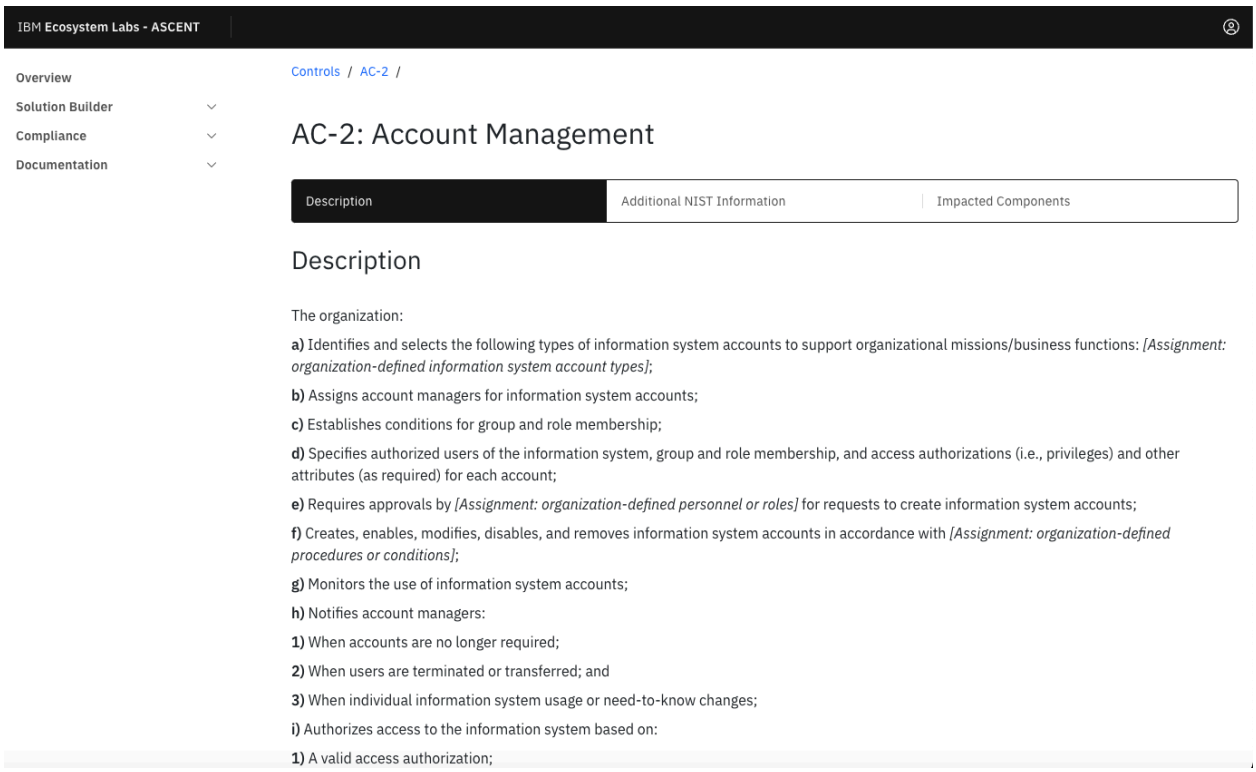


For IBM, Clients & Business Partner Use Only

15. Explain that controls are grouped into Control Families, navigating through the page of controls using the navigation at the bottom of the table show the controls and how they are aligned to control families.



16. At the top of the page search for control **AC-2 (**click on the search button and enter AC-2)
17. Click on the blue **AC-2** tag you will see the control detail



18. Scroll down through the control explain the control AC-2 Account management in more detail
19. Highlight the NIST guidance for the organization to implement this control
20. Highlight the Solution and Implementation guidance

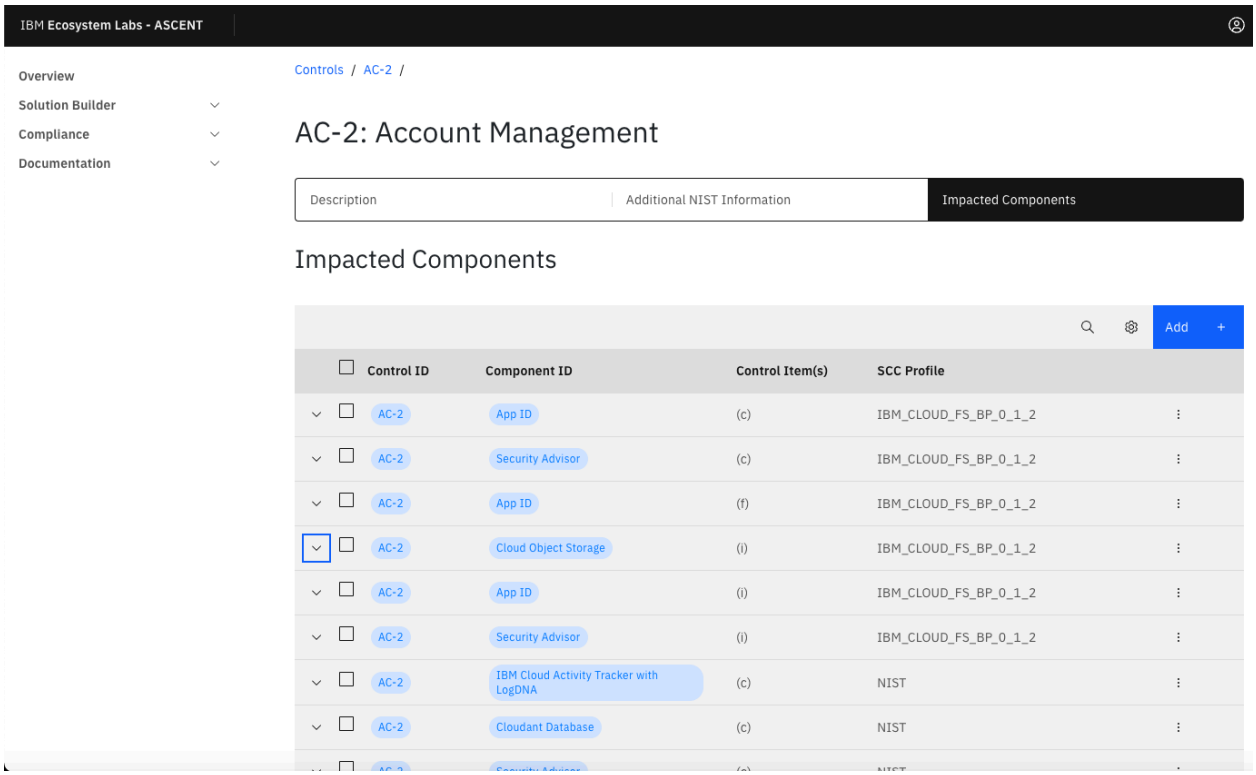
21. Highlight the control framework has Provider evidence on how you validate the control or sub control and the implementation guidance
22. Scroll back to the top and repeat this for several other controls for example **SC-11, etc.**
23. Using TechZone Deployer become familiar with the controls and explain the value of having this asset to help accelerate the on boarding of solutions into the FS Cloud.
24. Return back to the **AC-2** control and click on its detail view
25. Click on **Additional NIST Information** this will display the information that the NIST organization supplies to the industry navigate to this NIST website and click on AC-2

    a. https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&security_baseline=High
26. This will show you the sub controls as documented by the industry, and it will also so the control relationships
27. In the **TechZone Deployer** tool you can see the Priority and the relationships are listed in this view. Highlight the relationships to your audience.

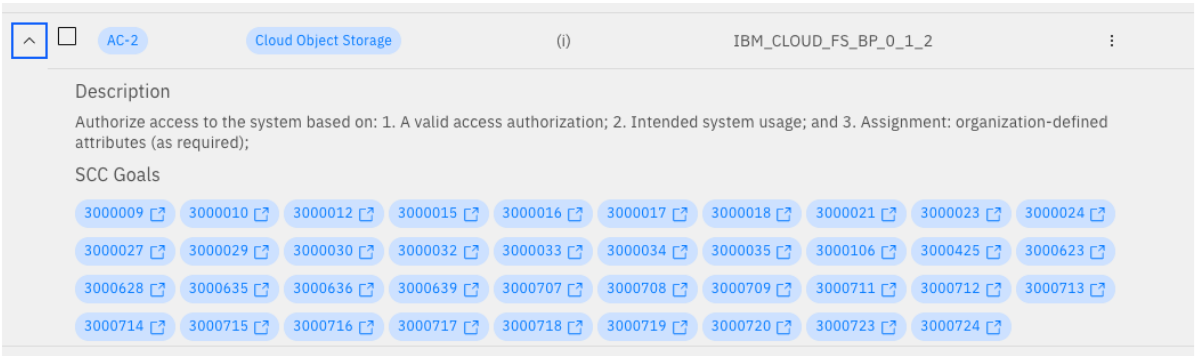
Controls Mapping how the FS Controls can be mapped to specific Cloud Services and then on to specific SCC goals in the Security and Compliance center.

Steps:

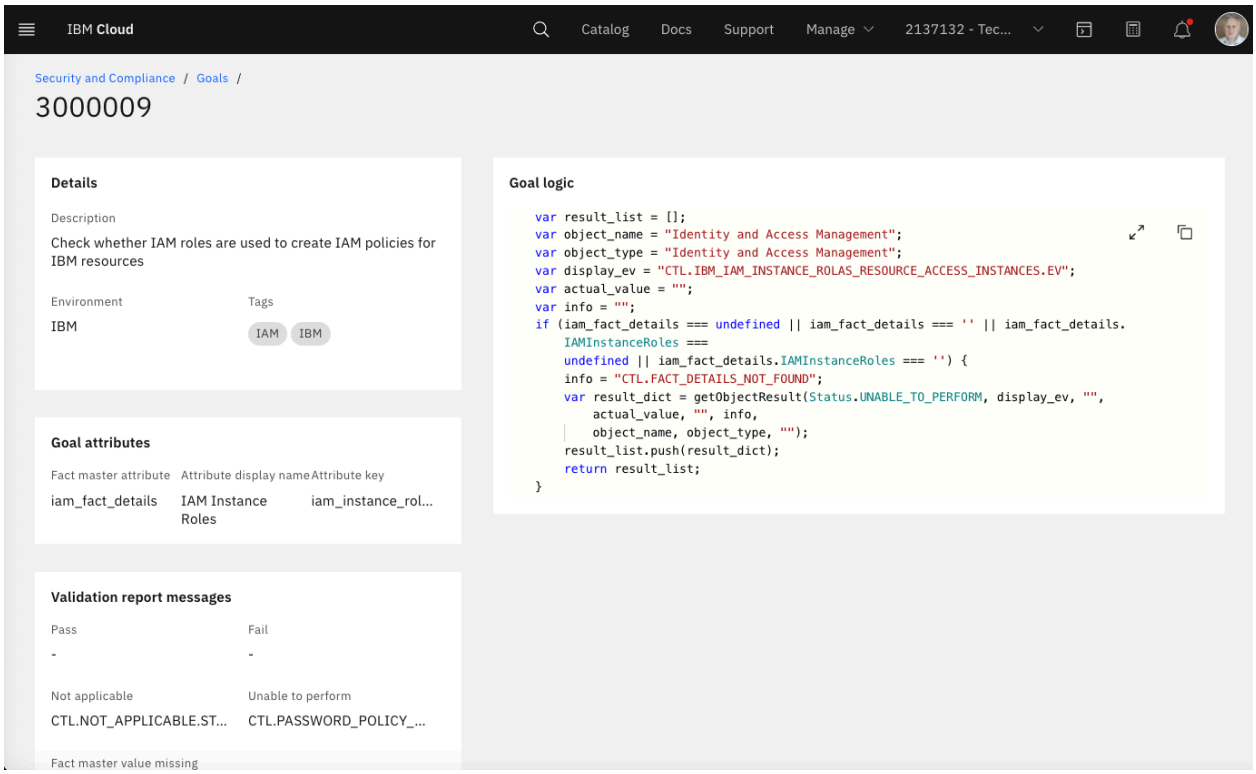
1. Log into **TechZone Deployer** tool using steps in previous section and navigate to **Compliance->Controls->AC-2 Detail View** and then select **Impacted Components.**



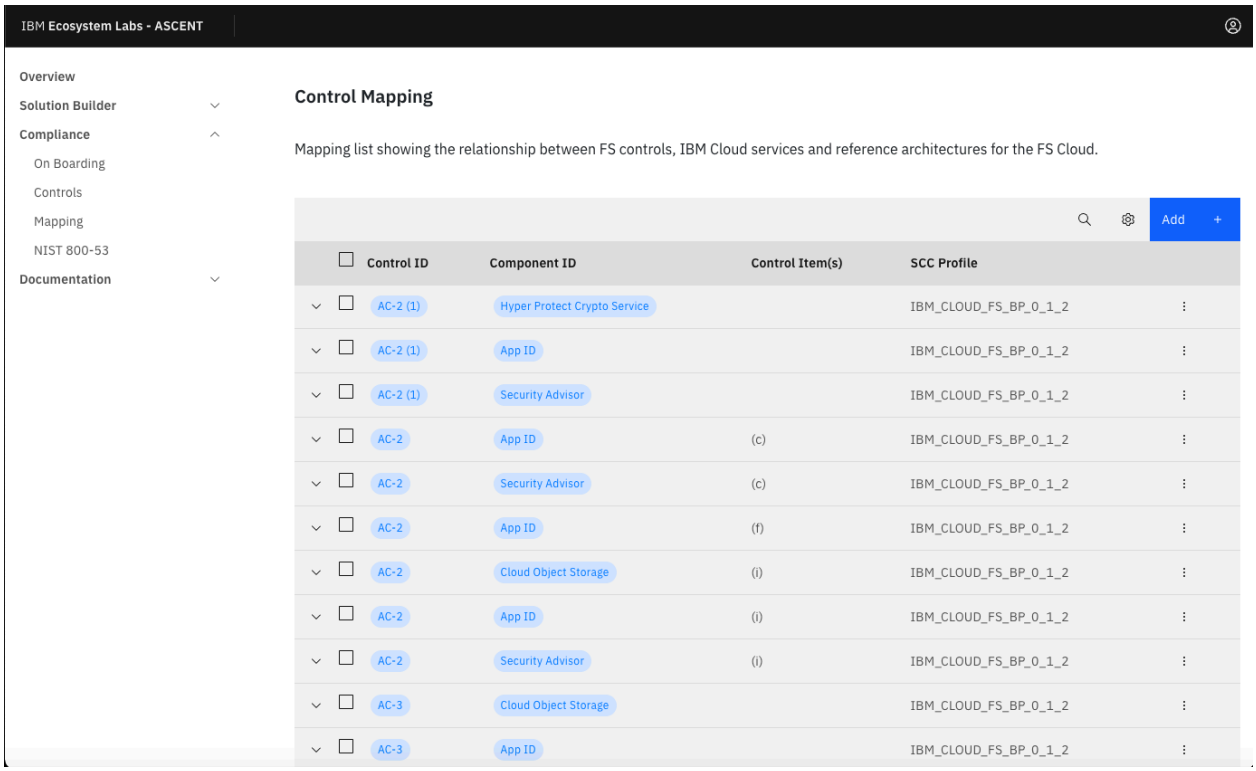
2. You will see all the Components (Cloud Services) that have a mapping relationship to the FS controls
3. In this case you can explain how **AC-2** has mapping to **AppID, Cloud Object Storage etc**
4. Expand the twisty on **AC-2->Cloud Object Storage**



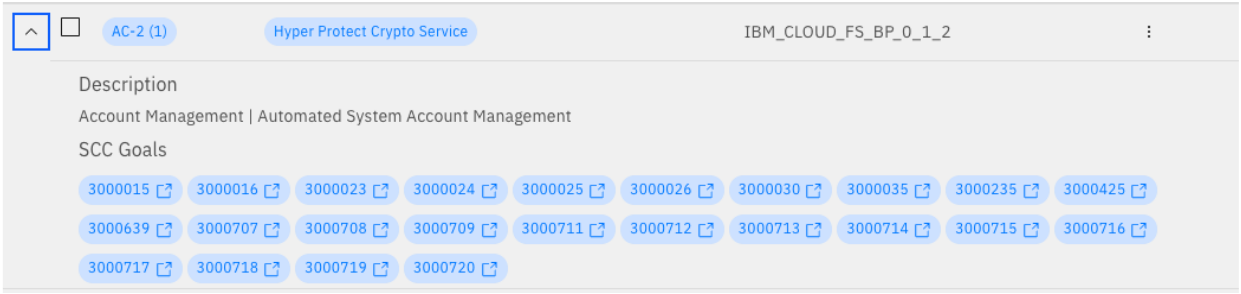
5. You can see all the Goals that have been mapped to the cloud service and how these goals map to the FS Control
6. Click on one of the Goals **3000009** (make sure you are logged into the TechZone Cloud Account)



7. You can see the Goal That Is defined to validate that the Multi Factor Authentication is enabled and aligned to the resource that is defined in the architecture.
8. Click on a few of the other goals to see how they related to the Cloud Object Storage services
9. Now you have explained the relationship from the Controls to the Cloud Services lets navigate to the mapping view
10. Click on **Compliance->Mapping**

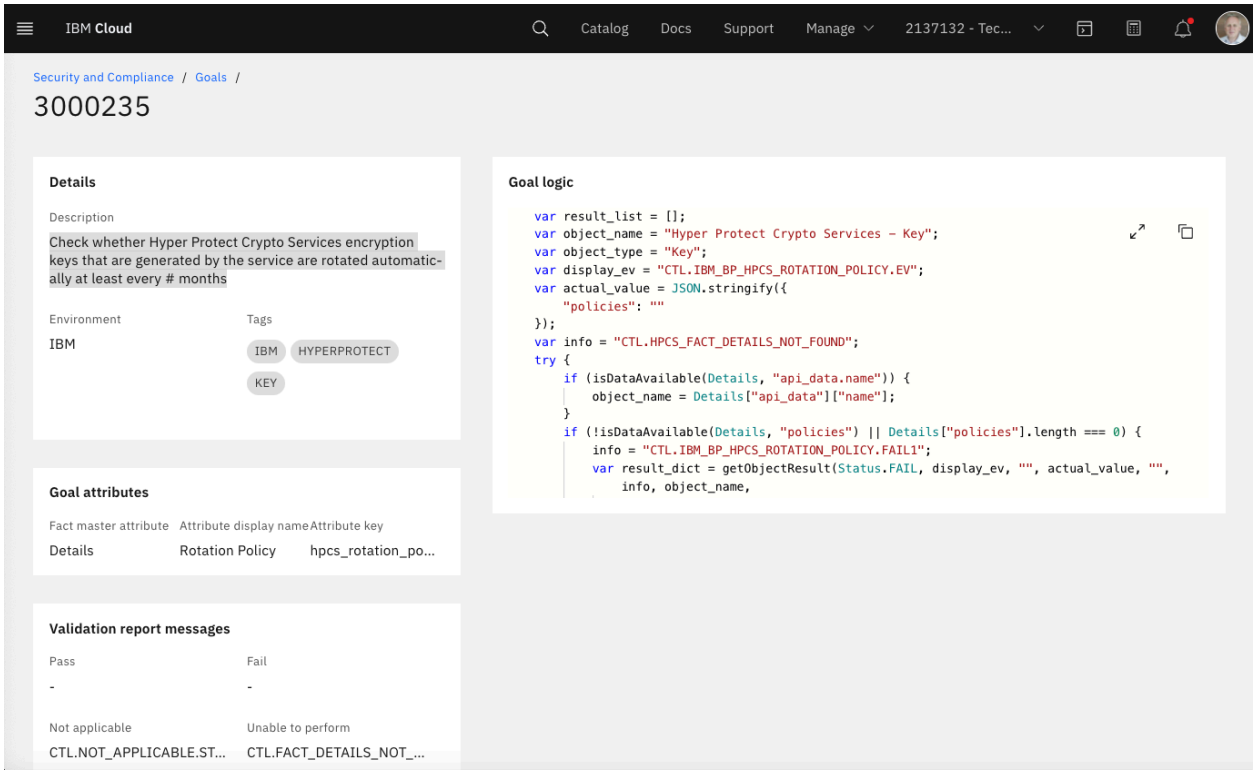


11. You can see the list of controls and how they map to the Cloud services. You can also see the SCC profile that was used to import the mapping data into the **TechZone Deployer** tool. This makes its clearer to explain the end-to-end relationships.
12. Expand the Hyper Protect Crypto Service and show the goals that are linked to this services

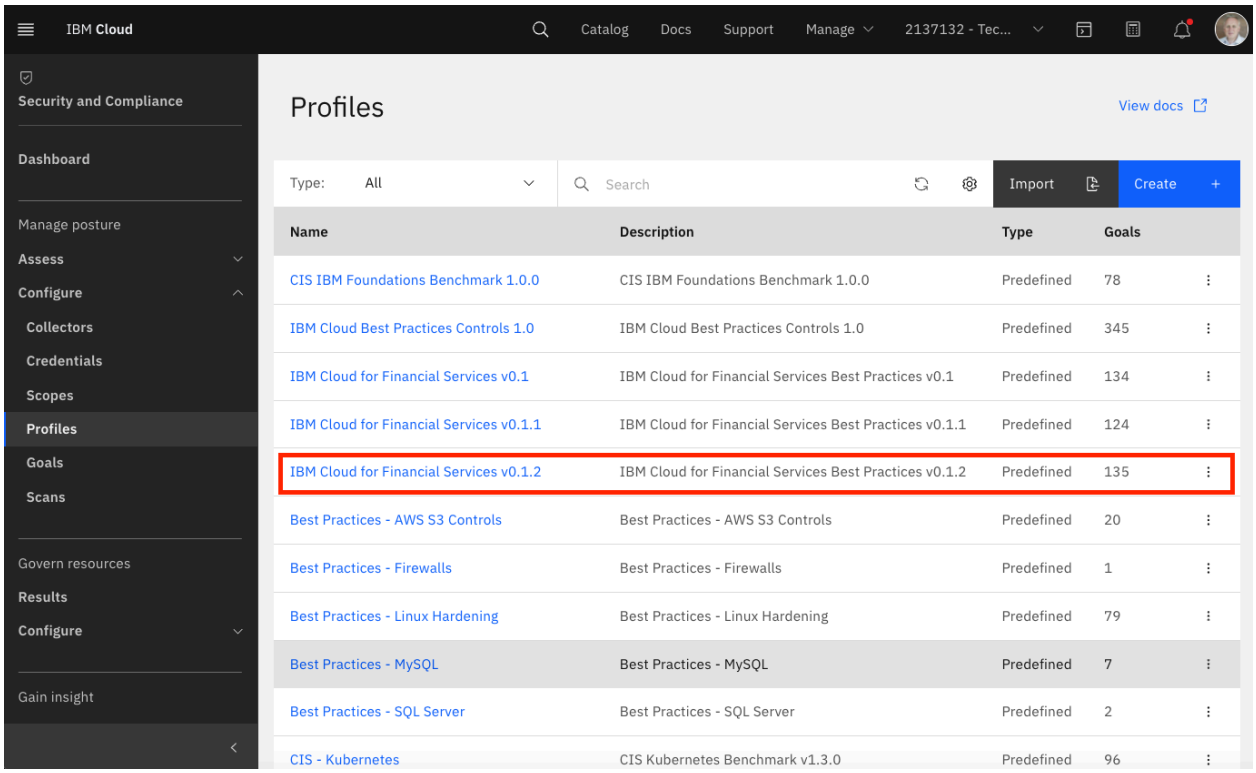


13. Explain the mapping to AC-2(1) control
14. Click on a few goals to show how they are implemented in the IBM Cloud console.
15. Open Goal **3000235** this goal highlights a key validation check.
    a. Check whether Hyper Protect Crypto Services encryption keys that are generated by the service are rotated automatically at least every # months

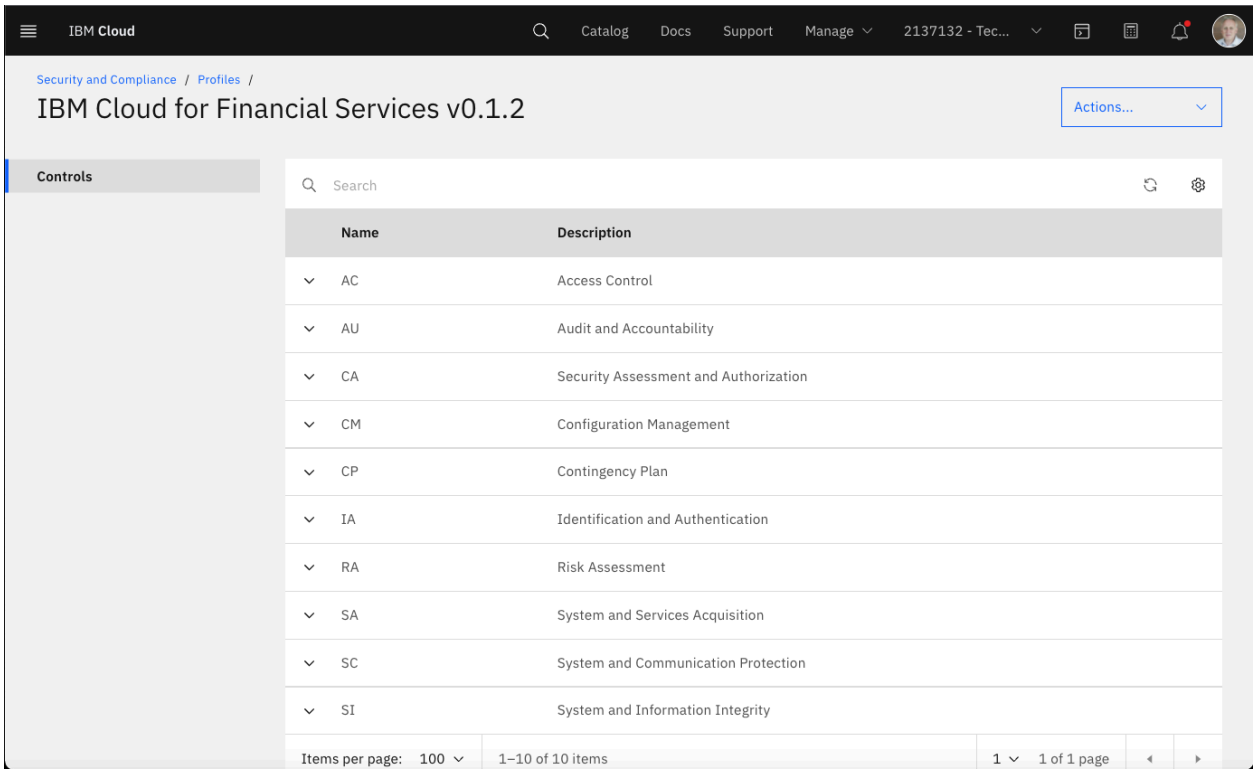
16. It's this level of validation from the cloud platform that enables the controls to be validated and reported to a compliance and risk teams.



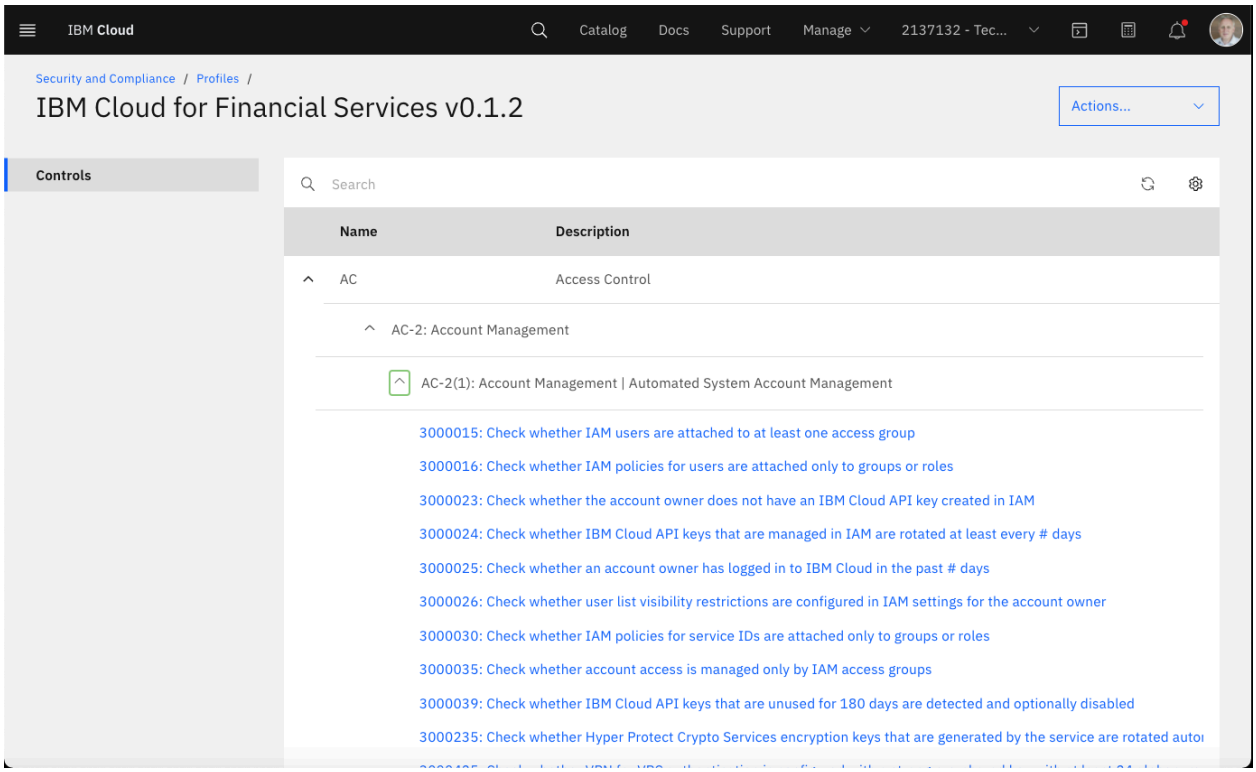
17. While in the IBM Cloud console click on **Menu->Security and Compliance->Configure->Profiles**



18. Click on the **IBM Cloud for Financial Services vX.X.X** this will open up the profile for Financial Services



19. You will see the FS Control families listed
20. Expand **AC – Access Control**
21. Expand **AC-2: Account Management**
22. Expand **AC-2(1): Account Management | Automated System Account Management**
23. You will see all the goals that are group into the specific FS Control



24. You can explain the relationships clearly now to the FS Control framework that discussed in the first section
25. Click on a few goals to navigate to them specifically

THIS CONCLUDES THE LAB STEPS