



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:

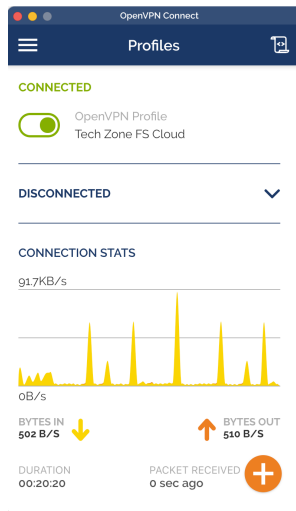
- If you have not already done so, request access to the FS Cloud demo environment at: <https://techzone.ibm.com/collection/ibm-cloud-for-financial-services>
- Download and install the OpenVPN client
 - Windows <https://openvpn.net/community-downloads/>
 - MacOS <https://openvpn.net/client-connect-vpn-for-mac-os/>
 - 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>



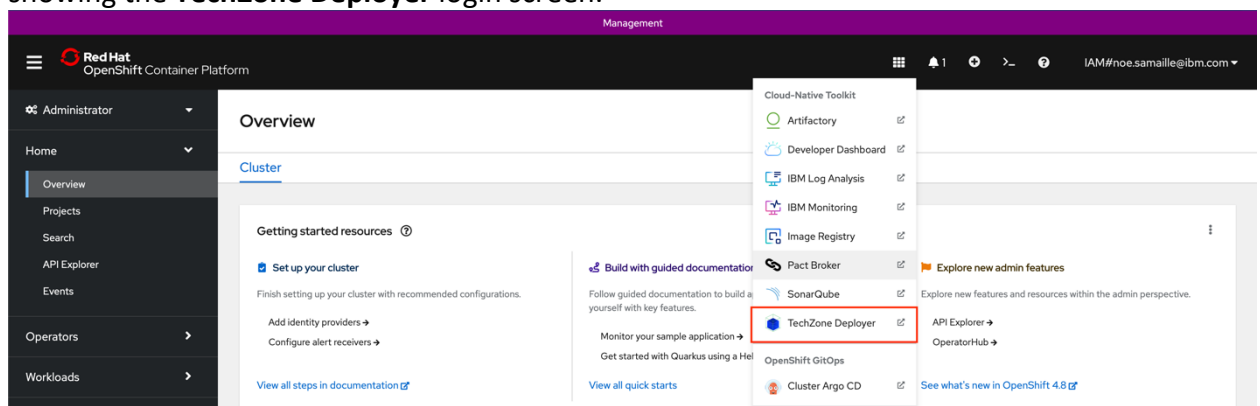
IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

Steps:

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



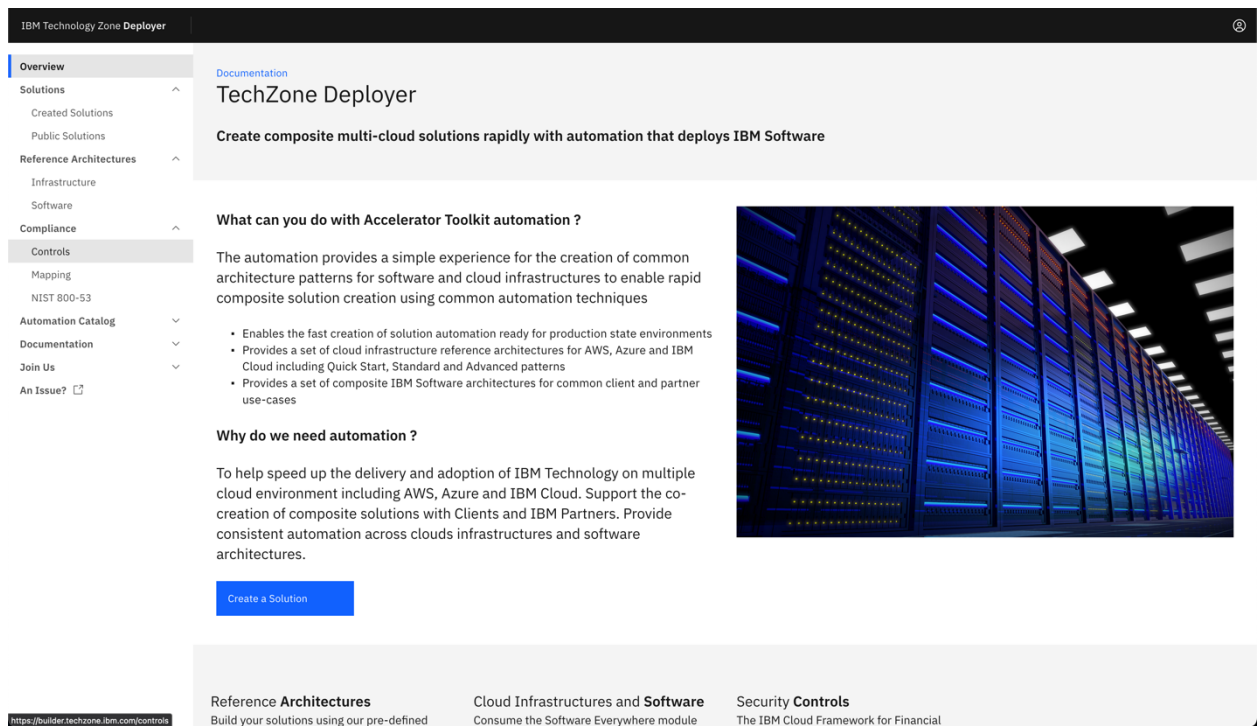
2. Login to IBM Cloud <https://cloud.ibm.com>
3. For official documentation of the IBM Cloud for Financial Services controls framework, navigate to <https://cloud.ibm.com/docs/framework-financial-services?topic=framework-financial-services-about>
4. In this lab, we will use an accelerator tool created 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.





IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

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



- On the menu on the left select **Compliance -> Controls** this will display the list of controls.
- Controls define the compliance requirements that a Risk team or Compliance officer will need the validate for a solution implemented on IBM Cloud.



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

IBM Technology Zone Deployer

Overview

Solutions

Created Solutions

Public Solutions

Reference Architectures

Infrastructure

Software

Compliance

Controls

Mapping

NIST 800-53

Automation Catalog

Documentation

Join Us

An Issue?

Controls

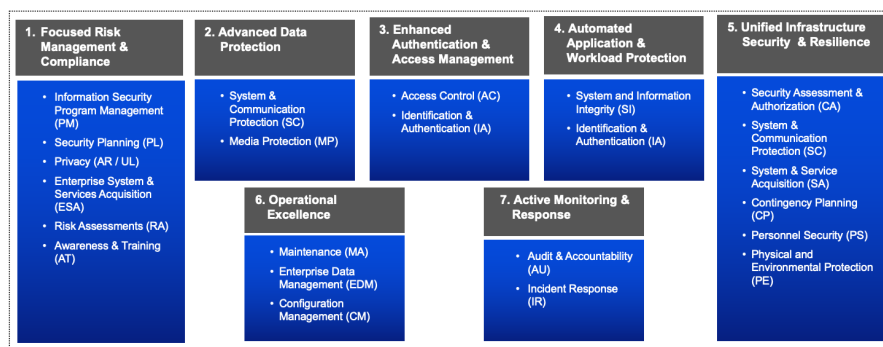
List of Controls defined for IBM Cloud for Financial Services (more info...)

Control ID	Focus Area	Control Family	Control Name	Parent Control
AC-1	#3 - Enhanced Authentication & Access Management	Access Control (AC)	Access Control Policy and Procedures	Base Control
AC-11	#3 - Enhanced Authentication & Access Management	Access Control (AC)	Session Lock	Base Control
AC-11 (1)	#3 - Enhanced Authentication & Access Management	Access Control (AC)	Session Lock Pattern-Hiding Displays	AC-11
AC-14	#3 - Enhanced Authentication & Access Management	Access Control (AC)	Permitted Actions Without Identification or Authentication	Base Control
AC-16	#3 - Enhanced Authentication & Access Management	Access Control (AC)	Security Attributes	Base Control
AC-17	#3 - Enhanced Authentication & Access Management	Access Control (AC)	Remote Access	Base Control
AC-17 (9)	#3 - Enhanced Authentication & Access Management	Access Control (AC)	Remote Access Disconnect / Disable Access	AC-17
AC-18	#3 - Enhanced Authentication & Access Management	Access Control (AC)	Wireless Access	Base Control
AC-19	#3 - Enhanced Authentication & Access Management	Access Control (AC)	Access Control For Mobile Devices	Base Control
AC-19 (5)	#3 - Enhanced Authentication & Access Management	Access Control (AC)	Access Control For Mobile Devices Full Device / Container-Based Encryption	AC-19

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.

IBM Cloud Framework for Financial Services Focus Areas and Control Alignment

Seven focus areas, 21 unique control families, ~280 controls



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.



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

CM-2	Baseline Configuration	Configuration Management	Base Control	Human	Setup	:
CM-2 (1)	CONTROL ENHANCEMENT	Configuration Management	CM-2	Human	Mix	:
CM-2 (2)	CONTROL ENHANCEMENT	Configuration Management	CM-2	Automated	Setup, Event	Next page
Items per page 15		61–75 of 278 items		5	of 19 pages	◀ ▶

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

IBM Ecosystem Labs - ASCENT

Controls / AC-2 /

Overview
Solution Builder
Compliance
Documentation

AC-2: Account Management

DescriptionAdditional NIST InformationImpacted Components

Description

The organization:

- a) Identifies and selects the following types of information system accounts to support organizational missions/business functions: *[Assignment: organization-defined information system account types]*;
- b) Assigns account managers for information system accounts;
- c) Establishes conditions for group and role membership;
- d) Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
- e) Requires approvals by *[Assignment: organization-defined personnel or roles]* for requests to create information system accounts;
- f) Creates, enables, modifies, disables, and removes information system accounts in accordance with *[Assignment: organization-defined procedures or conditions]*;
- g) Monitors the use of information system accounts;
- h) Notifies account managers:
 - 1) When accounts are no longer required;
 - 2) When users are terminated or transferred; and
 - 3) When individual information system usage or need-to-know changes;
- i) Authorizes access to the information system based on:
 - 1) A valid access authorization;

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



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

IBM Ecosystem Labs - ASCENT

Overview
Solution Builder
Compliance
Documentation

Solution and Implementation

Part a)

Provider Implementation Guidance

Identify types of accounts to support organizational missions/business functions. When specifying account types, the provider considers the following account types that apply for their IBM Cloud accounts, host operating systems, and applications: individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, service accounts, privileged administrator accounts, domain administrator accounts, local device accounts, and customer privileged administrative accounts.

An IBM Cloud account is required to create and manage IBM Cloud resources. Within an account, the account owner or their delegate can create an access group to organize a set of users and service IDs into a single entity and easily assign permissions. Accesses can be grouped into policies and applied to groups of users instead of assigning the same access multiple times per individual user or service ID.

Those individuals who are responsible for the development and operation of the production environment where provider is hosting the application should be assigned to an access group that is separate from the users who can order and configure services from the IBM Cloud console, command line interface (CLI), or application programming interface (PI) (e.g., the admin that is responsible for the configuration of encryption should not have the ability to write data within the environment because they could turn off encryption, write data, or turn on encryption (and thereby bypass encrypting data at rest and/or the administrator that is responsible for setting audit levels should not be able to perform actions within the application such as turning on/off audit or dump data. provider should have RBAC configured for all its staff enforcing separation of duties (SOD).

For additional information on IBM Cloud accounts, please refer to Overview of accounts, identity management, and access control.

The following provides additional context for the domains mentioned above:

- Provider operators:
 - IBM Cloud account users: Includes administrators whose function is to order resources to be used in the provider's deployment such as virtual private clouds (VPC), virtual servers, etc. and operators who need to access cloud resources for operations. IBM Cloud IAM can federate to the provider's identity provider (IdP).
 - Operating System (OS) operator/application account users: This is the domain that defines provider users with fewer privileges than administrators described above. These users may be operators who only need access to the OS level of the virtual machines (VM)/containers, application developers, testers, and other less-privileged roles relative to the operation of the IBM Cloud deployment itself.

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.



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

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**.

IBM Ecosystem Labs - ASCENT

Controls / AC-2 /

Overview
Solution Builder
Compliance
Documentation

AC-2: Account Management

Description | Additional NIST Information | **Impacted Components**

Impacted Components

<input type="checkbox"/>	Control ID	Component ID	Control Item(s)	SCC Profile	
<input checked="" type="checkbox"/>	AC-2	App ID	(c)	IBM_CLOUD_FS_BP_0_1_2	:
<input checked="" type="checkbox"/>	AC-2	Security Advisor	(c)	IBM_CLOUD_FS_BP_0_1_2	:
<input checked="" type="checkbox"/>	AC-2	App ID	(f)	IBM_CLOUD_FS_BP_0_1_2	:
<input checked="" type="checkbox"/>	AC-2	Cloud Object Storage	(i)	IBM_CLOUD_FS_BP_0_1_2	:
<input checked="" type="checkbox"/>	AC-2	App ID	(i)	IBM_CLOUD_FS_BP_0_1_2	:
<input checked="" type="checkbox"/>	AC-2	Security Advisor	(i)	IBM_CLOUD_FS_BP_0_1_2	:
<input checked="" type="checkbox"/>	AC-2	IBM Cloud Activity Tracker with LogDNA	(c)	NIST	:
<input checked="" type="checkbox"/>	AC-2	Cloudant Database	(c)	NIST	:

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**

☒ AC-2 Cloud Object Storage (i) IBM_CLOUD_FS_BP_0_1_2 :

Description
Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Assignment: organization-defined attributes (as required);

SCC Goals

3000009	3000010	3000012	3000015	3000016	3000017	3000018	3000021	3000023	3000024
3000027	3000029	3000030	3000032	3000033	3000034	3000035	3000106	3000425	3000623
3000628	3000635	3000636	3000639	3000707	3000708	3000709	3000711	3000712	3000713
3000714	3000715	3000716	3000717	3000718	3000719	3000720	3000723	3000724	



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

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)

The screenshot shows the IBM Cloud interface for a specific goal. The header includes the IBM Cloud logo, a search bar, and navigation links for Catalog, Docs, Support, and Manage. The user is logged in as '2137132 - Tec...'. The main content area is titled 'Security and Compliance / Goals / 3000009'.

Details

Description: Check whether IAM roles are used to create IAM policies for IBM resources

Environment: IBM

Tags: IAM, IBM

Goal attributes

Fact master attribute	Attribute display name	Attribute key
iam_fact_details	IAM Instance Roles	iam_instance_rol...

Validation report messages

Pass	Fail
-	-
Not applicable	Unable to perform
CTL.NOT_APPLICABLE.ST...	CTL.PASSWORD_POLICY_...

Fact master value missing

Goal logic

```
var result_list = [];  
var object_name = "Identity and Access Management";  
var object_type = "Identity and Access Management";  
var display_ev = "CTL.IBM_IAM_INSTANCE_ROLAS_RESOURCE_ACCESS_INSTANCES.EV";  
var actual_value = "";  
var info = "";  
if (iam_fact_details === undefined || iam_fact_details === '' || iam_fact_details.  
IAMInstanceRoles ===  
undefined || iam_fact_details.IAMInstanceRoles === '') {  
info = "CTL.FACT_DETAILS_NOT_FOUND";  
var result_dict = getObjectResult(Status.UNABLE_TO_PERFORM, display_ev, "",  
actual_value, "", info,  
object_name, object_type, "");  
result_list.push(result_dict);  
return result_list;  
}
```

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**



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

IBM Ecosystem Labs - ASCENT

Overview
Solution Builder
Compliance
On Boarding
Controls
Mapping
NIST 800-53
Documentation

Control Mapping

Mapping list showing the relationship between FS controls, IBM Cloud services and reference architectures for the FS Cloud.

<input type="checkbox"/>	Control ID	Component ID	Control Item(s)	SCC Profile	
✓ <input type="checkbox"/>	AC-2 (1)	Hyper Protect Crypto Service		IBM_CLOUD_FS_BP_0_1_2	:
✓ <input type="checkbox"/>	AC-2 (1)	App ID		IBM_CLOUD_FS_BP_0_1_2	:
✓ <input type="checkbox"/>	AC-2 (1)	Security Advisor		IBM_CLOUD_FS_BP_0_1_2	:
✓ <input type="checkbox"/>	AC-2	App ID	(c)	IBM_CLOUD_FS_BP_0_1_2	:
✓ <input type="checkbox"/>	AC-2	Security Advisor	(c)	IBM_CLOUD_FS_BP_0_1_2	:
✓ <input type="checkbox"/>	AC-2	App ID	(f)	IBM_CLOUD_FS_BP_0_1_2	:
✓ <input type="checkbox"/>	AC-2	Cloud Object Storage	(i)	IBM_CLOUD_FS_BP_0_1_2	:
✓ <input type="checkbox"/>	AC-2	App ID	(i)	IBM_CLOUD_FS_BP_0_1_2	:
✓ <input type="checkbox"/>	AC-2	Security Advisor	(i)	IBM_CLOUD_FS_BP_0_1_2	:
✓ <input type="checkbox"/>	AC-3	Cloud Object Storage		IBM_CLOUD_FS_BP_0_1_2	:
✓ <input type="checkbox"/>	AC-3	App ID		IBM_CLOUD_FS_BP_0_1_2	:

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

^ ☐ AC-2 (1) Hyper Protect Crypto Service IBM_CLOUD_FS_BP_0_1_2 :

Description
Account Management | Automated System Account Management

SCC Goals

3000015 3000016 3000023 3000024 3000025 3000026 3000030 3000035 3000235 3000425
3000639 3000707 3000708 3000709 3000711 3000712 3000713 3000714 3000715 3000716
3000717 3000718 3000719 3000720

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



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

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.

The screenshot displays the IBM Cloud console interface for configuring a goal. The top navigation bar includes the IBM Cloud logo, search, and various utility links. The main content area is titled 'Security and Compliance / Goals / 3000235'.

Details

Description: Check whether Hyper Protect Crypto Services encryption keys that are generated by the service are rotated automatically at least every # months

Environment: IBM

Tags: IBM, HYPERPROTECT, KEY

Goal attributes

Fact master attribute	Attribute display name	Attribute key
Details	Rotation Policy	hpcs_rotation_po...

Validation report messages

Pass	Fail
-	-
Not applicable	Unable to perform
CTL.NOT_APPLICABLE.ST...	CTL.FACT_DETAILS_NOT_...

Goal logic

```
var result_list = [];  
var object_name = "Hyper Protect Crypto Services - Key";  
var object_type = "Key";  
var display_ev = "CTL.IBM_BP_HPCS_ROTATION_POLICY.EV";  
var actual_value = JSON.stringify({  
  "policies": ""  
});  
var info = "CTL.HPCS_FACT_DETAILS_NOT_FOUND";  
try {  
  if (isDataAvailable(Details, "api_data.name")) {  
    object_name = Details["api_data"]["name"];  
  }  
  if (!isDataAvailable(Details, "policies") || Details["policies"].length === 0) {  
    info = "CTL.IBM_BP_HPCS_ROTATION_POLICY.FAIL";  
    var result_dict = getObjectResult(Status.FAIL, display_ev, "", actual_value, "",  
      info, object_name,  
    );  
  }  
}
```

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



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

The screenshot shows the IBM Cloud console interface. The left sidebar is dark-themed and contains a list of navigation items. The main content area is titled 'Profiles' and features a table of predefined profiles. The profile 'IBM Cloud for Financial Services v0.1.2' is highlighted with a red rectangular box.

Name	Description	Type	Goals
CIS IBM Foundations Benchmark 1.0.0	CIS IBM Foundations Benchmark 1.0.0	Predefined	78
IBM Cloud Best Practices Controls 1.0	IBM Cloud Best Practices Controls 1.0	Predefined	345
IBM Cloud for Financial Services v0.1	IBM Cloud for Financial Services Best Practices v0.1	Predefined	134
IBM Cloud for Financial Services v0.1.1	IBM Cloud for Financial Services Best Practices v0.1.1	Predefined	124
IBM Cloud for Financial Services v0.1.2	IBM Cloud for Financial Services Best Practices v0.1.2	Predefined	135
Best Practices - AWS S3 Controls	Best Practices - AWS S3 Controls	Predefined	20
Best Practices - Firewalls	Best Practices - Firewalls	Predefined	1
Best Practices - Linux Hardening	Best Practices - Linux Hardening	Predefined	79
Best Practices - MySQL	Best Practices - MySQL	Predefined	7
Best Practices - SQL Server	Best Practices - SQL Server	Predefined	2
CIS - Kubernetes	CIS Kubernetes Benchmark v1.3.0	Predefined	96

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



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

The screenshot shows the IBM Cloud for Financial Services v0.1.2 interface. The top navigation bar includes the IBM Cloud logo, a search icon, and links to Catalog, Docs, Support, and Manage. The main header displays the title 'IBM Cloud for Financial Services v0.1.2' and an 'Actions...' button. The left sidebar is labeled 'Controls'. The main content area features a search bar and a table of controls.

Name	Description
AC	Access Control
AU	Audit and Accountability
CA	Security Assessment and Authorization
CM	Configuration Management
CP	Contingency Plan
IA	Identification and Authentication
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communication Protection
SI	System and Information Integrity

At the bottom of the table, there is a pagination bar showing 'Items per page: 100', '1-10 of 10 items', and '1 of 1 page'.

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



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

Security and Compliance / Profiles /

IBM Cloud for Financial Services v0.1.2

Actions...

Controls

Search

Name	Description
AC	Access Control
AC-2: Account Management	
AC-2(1): Account Management Automated System Account Management	
3000015:	Check whether IAM users are attached to at least one access group
3000016:	Check whether IAM policies for users are attached only to groups or roles
3000023:	Check whether the account owner does not have an IBM Cloud API key created in IAM
3000024:	Check whether IBM Cloud API keys that are managed in IAM are rotated at least every # days
3000025:	Check whether an account owner has logged in to IBM Cloud in the past # days
3000026:	Check whether user list visibility restrictions are configured in IAM settings for the account owner
3000030:	Check whether IAM policies for service IDs are attached only to groups or roles
3000035:	Check whether account access is managed only by IAM access groups
3000039:	Check whether IBM Cloud API keys that are unused for 180 days are detected and optionally disabled
3000235:	Check whether Hyper Protect Crypto Services encryption keys that are generated by the service are rotated autoi

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