FINOS

Fintech
Open Source
Foundation

Cloud Service Accelerator

Jonathan Meadows
Jason Nelson
JPMorgan Chase

January 24th, 2019

Cloud Controls Certification: Proposal Overview

- Project / Working Group Name: Cloud Controls Certification Working Group
- Project / Working Group Description: Define and codify cloud controls, providing secure default implementations with associated tests to prove control efficacy
- Program: FDX – FinServ Developer Experience
- Initial Contributors:
  - JPMorgan; looking for others
- Milestones
  - Review and release initial set of service accelerators including detailed control definition, sample implementation and test suite for AWS
  - Engage other Cloud Service Providers to provide implementation and satisfy tests for initial body of work
  - Engage Cloud Service Providers to implement additional accelerators across service offerings (Long Term)

Value for the Community

Current State before this project

- **Majority of cloud security incidents due to misconfiguration:** Services are not secure by default, configuration is often complex, nuanced and difficult to validate.
- **All financial institutions are re-inventing the wheel**: Institutions have similar control frameworks, we are all trying to secure and stand up the same providers and services.
- **This takes significant time and resources, delaying innovation**: 6 - 18 months elapsed time, every institution is fact finding with cloud providers
- **Results vary:** No guidance on how to implement controls, in-depth cloud service knowledge required to deliver this, we are not the cloud provider security experts

Proposed State with this project

- **Set quality standards across artefacts:** Members of all tiers can contribute to the project and ensure a common high level of quality is delivered and in less time.
- **Encourage cloud vendors to produce more industry specific content:** Member Participation and public release of the Accelerators will encourage cloud vendors to project more focused and quality content for Financial Services Industry.

Activity Evolution in the Foundation

- Near-term focus of the Program:
  - Define standard common set of controls
  - Review existing body of work - control definitions and implementations with working group members, amending to meet above controls
  - Release service accelerators to community, incorporating updates
  - Engage other Cloud Service Providers for contribution - Google, Azure

Requests for FINOS Member and Community

- Members
  - Collaboration: Request collaboration to review the existing body of work, defining standard controls and contribute with feedback regarding the best practice implementation provided
  - Communication to other Financial institutions and regulators: Raise awareness with other institutions to contribute and influence cloud service providers to extend to other services.
  - Participation: Present controls, sample implementations and test cases to regulators as standard approach to securely configure services?
- Community at-large
  - Awareness: Raise awareness of work to reduce duplication, applying pressure to Cloud Service Providers in order to provide standardised details for future service offerings
  - Collaboration: Extended contributions would be appreciated, incorporating amendments to sample implementation of controls

Cloud Service Accelerators: Problem Statement

- **Members strive to use services provided by AWS, Azure and Google to meet business demands for the cloud**
- **To do so requires each provider & service to be configured and implemented in a way that meets existing regulatory and internal controls.**

  - **All financial institutions are re-inventing the wheel**: Institutions have similar control frameworks, we are all trying to secure and stand up the same providers and services.
  - **This takes significant time and resources, delaying innovation**: 6 - 18 months elapsed time, every institution is fact finding with cloud providers
  - **Results vary…:** No guidance on how to implement controls, in-depth cloud service knowledge required to deliver this, we are not the cloud provider security experts

Cloud Service Accelerators: Solution / Artefacts

- **Define & codify standard controls, providing BDD style test cases to prove efficacy**
  - **Define standard control questions for cloud service**: Prior art here - Cloud Security Alliance Cloud Controls Matrix (CCM), EU-CERT initiative
  - **Reference security document:** Document to provide detailed guidance on implementation, answering standard process questions for compliance and security review
  - **Implementation of service to meet controls**: Write infrastructure as code to stand up service and meet control objectives (Terraform or platform agnostic code)
  - **Test cases to prove efficacy:** BDD test cases to prove efficacy of controls

Cloud Service Accelerators: Work so far

- We have implemented this work across 8 major AWS services.
- AWS now stated they will start to provide basic accelerators back to financial institutions
- By working with FINOS we can:
  - Set quality standards across artefacts
  - Extend to other cloud providers
  - Encourage cloud vendors to produce more industry specific content
  - Stop re-inventing the wheel!

Cloud Service Accelerators: Security Questions

Security Domain	Control Standard	BDD Test Scenario
Encryption		
Encryption of data at-rest (Ctrl 123)	Must ensure that end-to-end encryption is implemented such that data is encrypted at-rest and in-transit at all times. Std: 123)	Scenario: User attempts to save data without specifying encryption, should be rejected (or enforce encryption - to confirm) Scenario: User attempts to save data specifying SSE-S3 encryption, should be rejected Scenario: User attempts to save data specifying SSE-C encryption, should be rejected Scenario: User saves data to S3 bucket, validate that the cloud trail logs are updated appropriately Scenario: User creates cfn for an S3 bucket and does not reference SSE-KMS encryption, SDLC should reject the cfn Scenario: Validate encrypted objects being stored (store a known object to S3, pull HEAD object and check the KMS key ID or compare MD5 of plaintext vs ETag of the encrypted object (above and beyond - nice to have)

- The example control requirement is not unique to a single bank.
- This approach is the major change
- By having a common development to common controls it would be possible to reduce duplicated work across the industry

Cloud Service Accelerators: Reference Security Document

Security Domain	Control & Architectural Suggestions	References
Encryption		
Encryption of data in-transit (Ctrl 124)	To support SSL connections, Amazon Redshift creates and installs an AWS Certificate Manager (ACM) issued SSL certificate on each cluster. The set of Certificate Authorities that you must trust in order to properly support SSL connections can be found at https://s3.amazonaws.com/redshift-downloads/redshift-ca-bundle.crt. RedShift endpoints are available over HTTPS at a selection of regions. Best practice: Set the **"require_SSL"** parameter to **"true"** in the parameter group that is associated with the cluster. For workloads that require FIPS-140-2 SSL compliance an additional step is required to set parameter **"use_fips_ssl"** to **"true"**	1. How to encrypt end to end: https://aws.amazon.com/blogs/big-data/encrypt-your-amazon-redshift-loads-with-amazon-s3-and-aws-kms/ 2. To make client side encryption work follow this pattern https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html 3. https://docs.aws.amazon.com/acm/latest/userguide/import-certificate.html

Cloud Service Accelerators: Implementation (Infrastructure as Code)

```
{
 "AWSTemplateFormatVersion": "2010-09-09",
 "Description": "Amazon DynamoDB Template",
 "Metadata": {
  "AWS::CloudFormation::Interface": {
   "ParameterGroups": [
    {
     "Label": {
      "default": "DynamoDB Table Settings"
     },
     "Parameters": [
      "pTableName",
      "pSSESpecification",
      "pHashKeyElementName",
      "pHashKeyElementType",
      "pReadCapacityUnits",
      "pWriteCapacityUnits"
     ]
    }
   ],
   "ParameterLabels": {
    "pHashKeyElementName": {
     "default": "Partition Key Name"
    },
    "pHashKeyElementType": {
     "default": "Partition Key Type"
    },
    "pReadCapacityUnits": {
     "default": "Read Capacity"
    },
    "pWriteCapacityUnits": {
     "default": "Write Capacity"
```

- Infrastructure as code

- Provides single common way to implement architectures
- Allows for common method to evaluate for efficacy alongside the rest of applications being deployed
- Code can be managed and secured
- Code is what is audited and moves compliance and security earlier in the development lifecycle

Cloud Service Accelerators: BDD Test Cases

```
Feature: Create the SQS Cfn stacks in the correct region
  Test that we can create the right SQS stack correctly in US and non-US region
  Scenario Outline: Create the SQS Cfn stack in US and non-US regions
    Given that I have valid AWS credentials with privileges to use CloudFormation
    When I try to deploy the <regional> SQS stack in <region>
    Then the stack creation should <result>

    Examples:
      | regional | region      | result    |
      | US       | us-east-1   | SUCCEED   |
      | Non-US   | eu-west-1   | SUCCEED   |
      | US       | eu-west-1   | FAIL      |
      | Non-US   | us-east-1   | FAIL      |

Scenario: Change permissions on a queue that I do not have access to
            Given that I have valid AWS credentials with permission to use SQS
            And I have IAM permissions to read, write and modify an SQS queue
            And I have IAM permissions to read, write and modify an SQS queue
            And the queue access policy allows me to read, write and modify the SQS queue
            When I try to change permissions on a queue that I do not have access to
            Then it should fail
```

- Can be tested, like code
- Provides high level of assurance that infrastructure as code is effective and performs as expected using Behavior Driven Develop (BDD) test cases.
- This level of evaluation has yielded discovery of inefficacy of proposed controls that manual review did not.
- Having verifiable and automated tests has enabled legacy security and audit process to mature more rapidly and trust BDD results as basis for audit.

FINOS

Fintech
Open Source
Foundation

Join our Community today!

finos.org/programs
finos.org/become-a-member

1117 So. California Avenue
Palo Alto, CA 94304
+1 650.665.9773
info@finos.org