Secure By Design: Codified Controls For Cloud Services

This talk will introduce the idea and method used by JPMorgan Chase & Co. to get cloud services approved for use in an accelerated timeline. This idea and method are now a project at FINOS and will use the collective efforts of members to build codified...
FINOS Project

Financial Delivery Accelerator (FDX) – Cloud Service Certification
Where to find it:

Github: https://github.com/finos-fdx/cloud-service-certification

Google Group: https://groups.google.com/a/finos.org/forum/#!forum/fdx-cloud-service-certification

Wiki: https://finosfoundation.atlassian.net/wiki/spaces/FDX/pages/904626436/Cloud+Service+Certification+Working+Group
Using Cloud Services at a Bank

• On-premise security controls must be adjusted for cloud security models
• How to map control frameworks to cloud service implementation?
• How to change a culture of NO into a culture of Yes.
Why are accelerators needed?

• 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
We built a process to solve a problem.

- How do you know your process is broken?
- Why do accelerators solve for the problem?
- What does it look like?
What artifacts make an accelerator?

- 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
## Define standard control questions for cloud service

<table>
<thead>
<tr>
<th>Security Domain</th>
<th>Control Standard</th>
<th>BDD Test Scenario</th>
</tr>
</thead>
</table>
| Encryption            | **Encryption of data at-rest** Must ensure that end-to-end encryption is implemented such that data is encrypted at-rest and in transit at all times. | **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) |
## Encryption

<table>
<thead>
<tr>
<th>Security Domain</th>
<th>Control &amp; Architectural Suggestions</th>
<th>References</th>
</tr>
</thead>
</table>
| Encryption               | To support SSL connections, Amazon Redshift creates and installs an [AWS Certificate Manager (ACM)](https://aws.amazon.com/security/certificate-manager/) 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](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/](https://aws.amazon.com/blogs/big-data/encrypt-your-amazon-redshift-loads-with-amazon-s3-and-aws-kms/)  
Implementation of service to meet controls

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

• Changes how your project management approach defines work
• Defines in simple full sentences the needed outcome of the work
• Can be tested, like code
• Example Please?
What is BDD?

Feature: Kinesis Data Streams is set up with the right security controls
Tests that Kinesis Data Streams have security controls enabled

Scenario: Connect to Kinesis over an unencrypted connection
Given that I have valid AWS credentials with permissions to use Kinesis Data Streams
And I have IAM permissions to read, write and modify a Kinesis Data Stream
When I try to send data to Kinesis without using encryption
Then it should fail
We built a tool to solve a problem.

• Why build when you can buy?
• How do you know you have a secure by design approach?
• How do you integrate BDD into your SDLC?
We made changes along the way

• Building it yourself is not always the best idea
End results

• We were able to observe shorter time from use case to service approval.

• Having a structured approach enables cloud services adoption at a more rapid pace.

• Using code for controls allowed for reuse instead of reinvention.
Q&A
FINOS Project

Financial Delivery Accelerator – Cloud Service Certification
Where is this project?

Github: https://github.com/finos-fdx/cloud-service-certification

Google Group: https://groups.google.com/a/finos.org/forum/#!forum/fdx-cloud-service-certification

Wiki: https://finosfoundation.atlassian.net/wiki/spaces/FDX/pages/904626436/Cloud+Service+Certification+Working+Group
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 set of controls to satisfy common framework requirements
  - 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
Outcomes and Impact

- **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.
Thank you for your attendance.