FINOS Common Cloud Controls

Jon Meadows – Citi Tech Fellow

August 3rd 2023

Agenda

A Quick Recap

More Detail on major components of CCC

Working Groups & Next Steps

A recap - The need for a Financial Services Public Cloud Standard

Why is this important?

- CSP differentiation makes regulatory, operational and cyber resilience complicated, bespoke and costly…
- …but our regulators are increasingly moving towards establishing and enforcing technical standards

Why is this important to FINOS members?

- The buck stops with us! CSPs are not responsible for institutional risk management, we are!
- FINOS members have the institutional knowledge to develop an *appropriate* Cloud standard, and the critical mass to work with CSPs to drive adoption

What is being proposed?

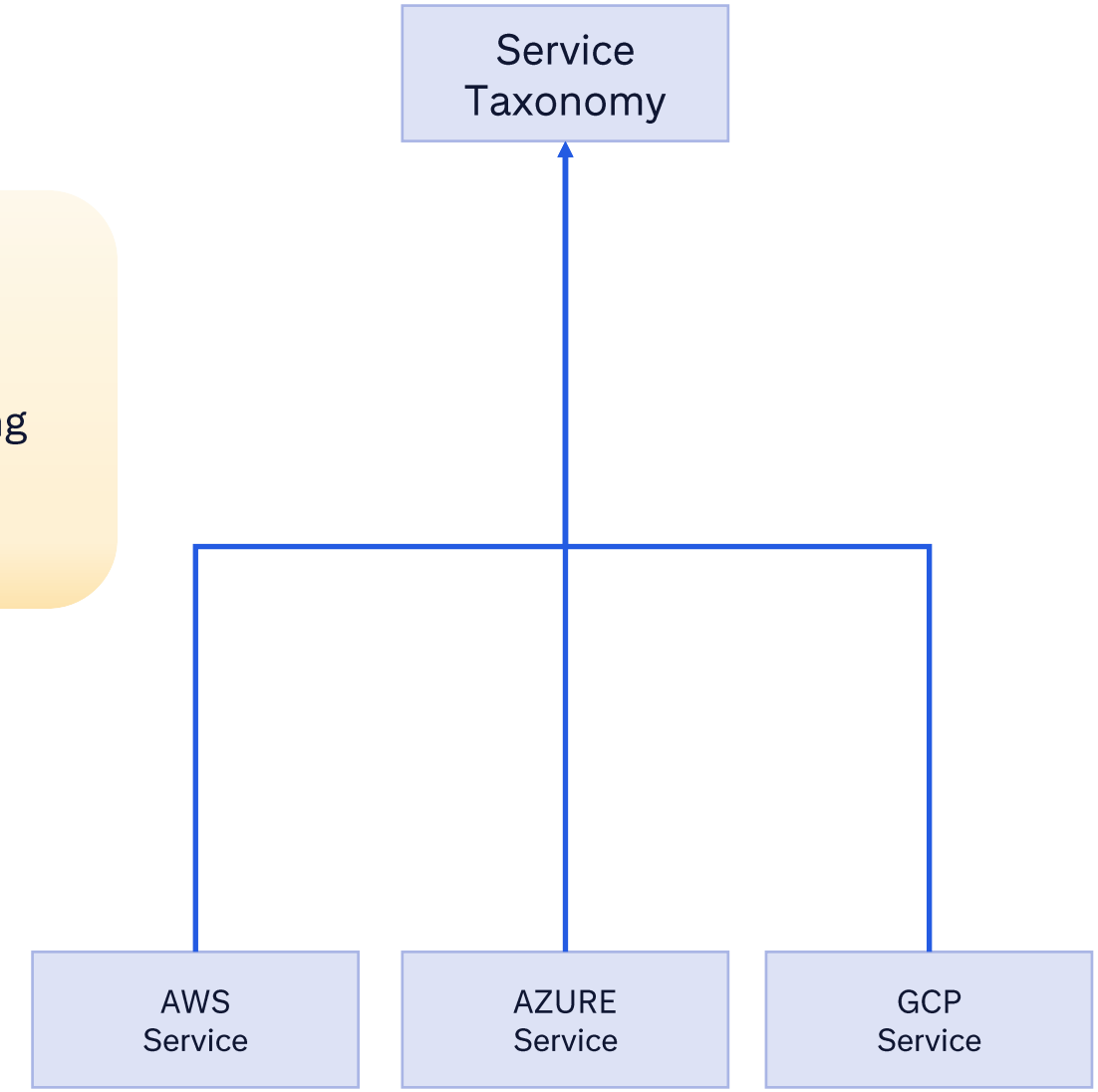
- The proposed *Financial Services Common Cloud Controls (C^3)* would be an industry standard that describes consistent controls for a *subset of CSP services* that are common across CSPs and are fundamental to most solutions
- CSPs would certify themselves against the standard in a machine-verifiable way
- Various regulators can map their requirements to a single consistent standard, a public cloud regulatory "Rosetta Stone"

citi

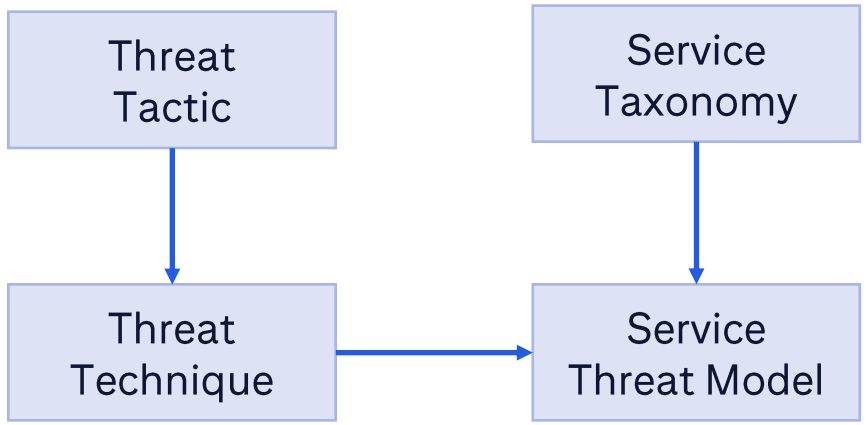
C^3 – Main Components: Service Taxonomy

Definitions of service types.

Important when looking to share threat models between CSP's



C^3 – Main Components: High Level Threat Model



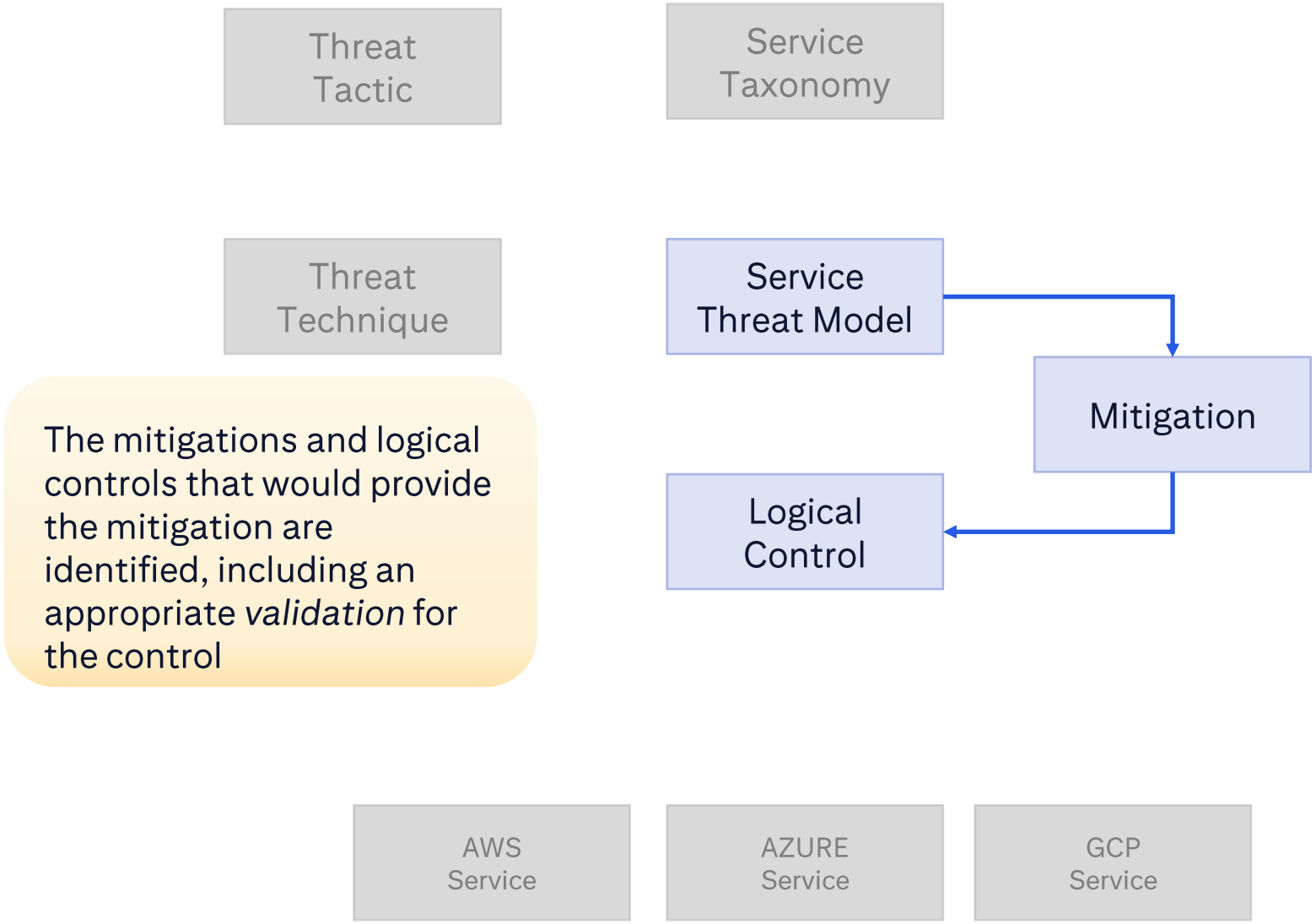
Leveraging the MITRE ATT&CK Framework and common architecture approach, a Threat Model for the generalized service is created.

AWS Service

AZURE Service

GCP Service

C³ – Main Components: Control Definition



C3 – Putting it all together

Threat Tactic

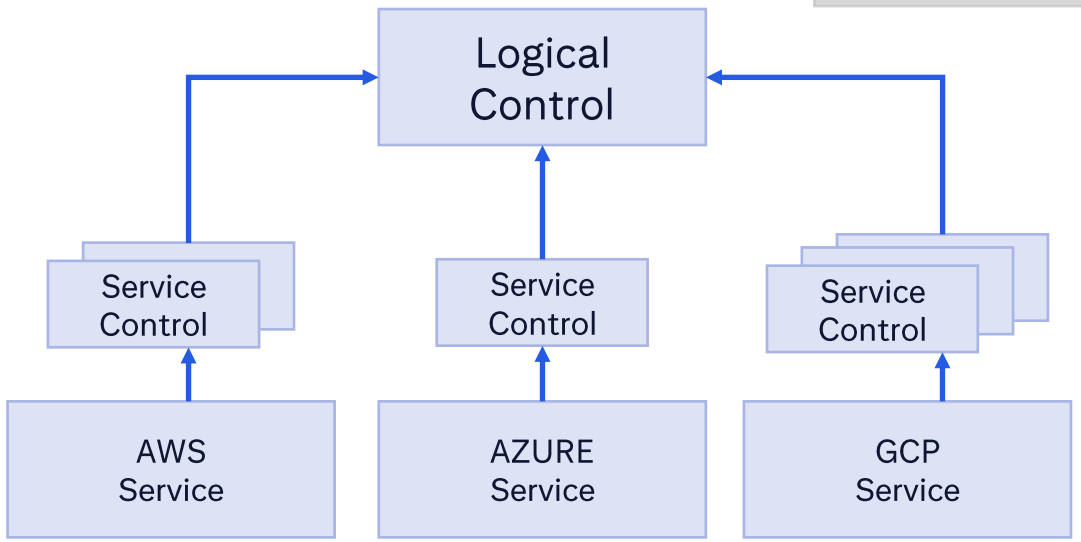
Service Taxonomy

Threat Technique

Service Threat Model

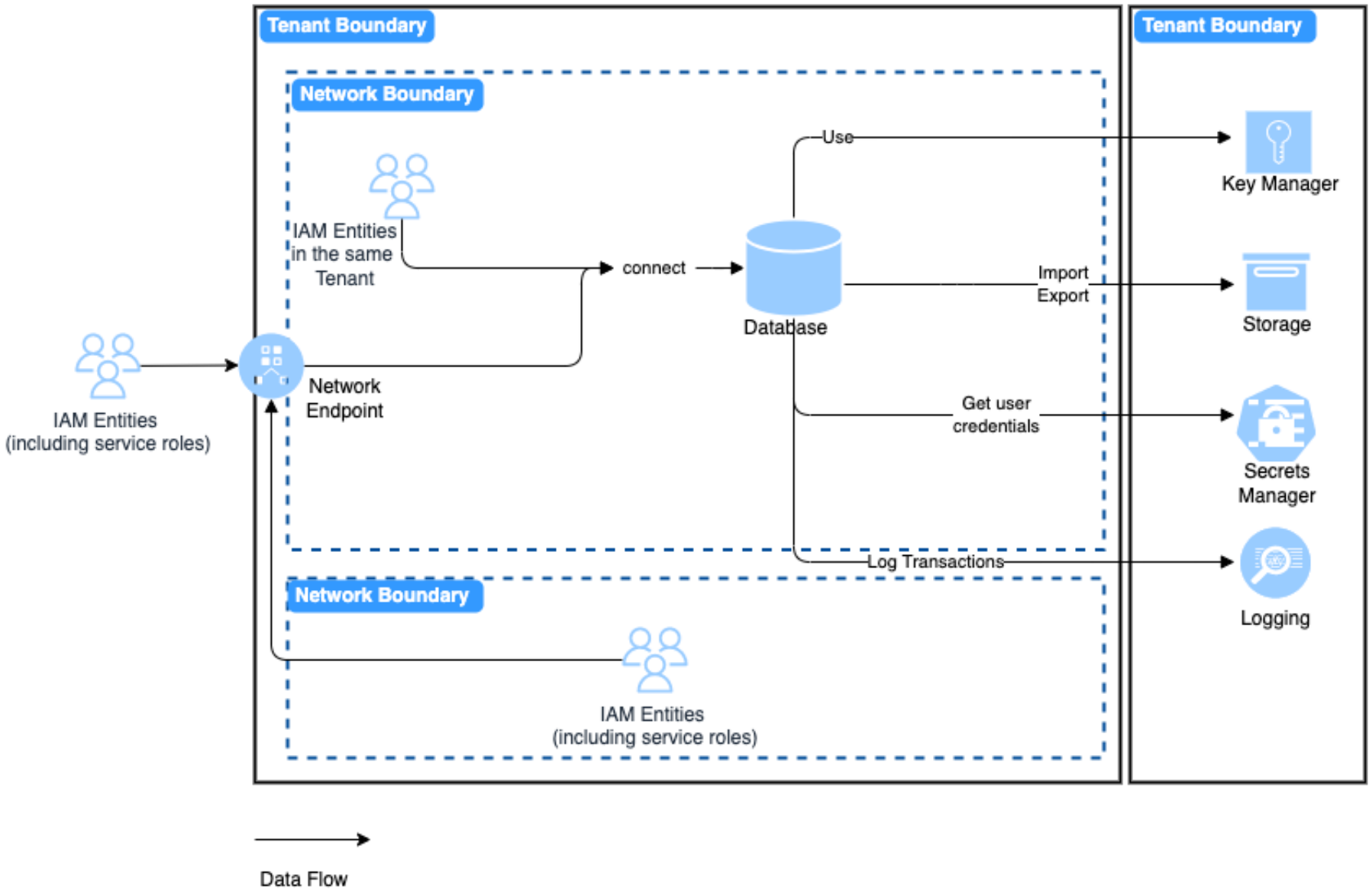
Mitigation

Each CSPs can provide the control implementations specific to their service which can satisfy the conditions of the logical control

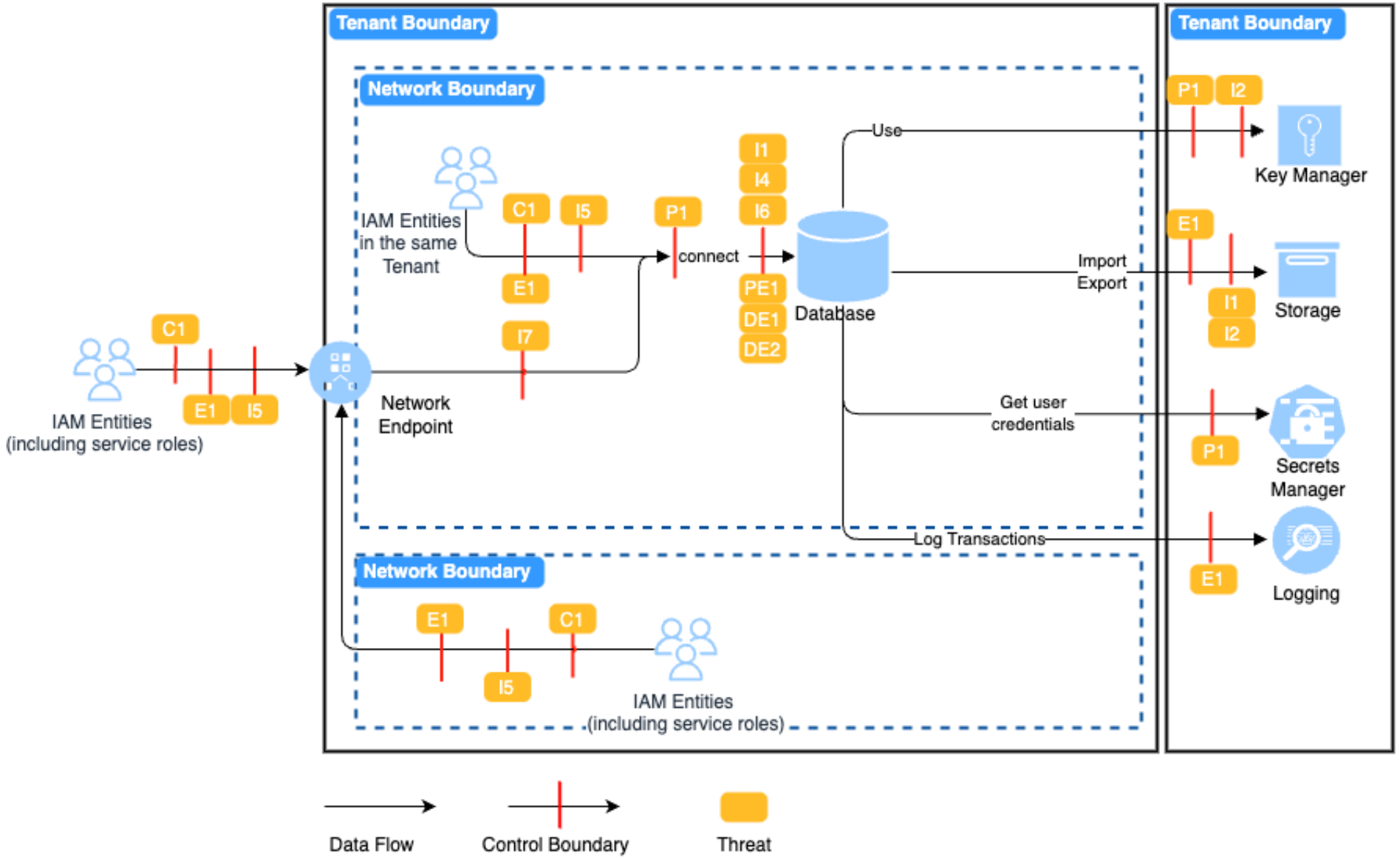


...with these services considered compliant to the C3 standard for that service

High Level Generic Data-Flow for Relational Database



High Level Threats Represented in Data-Flow for Relational Database



Documenting High Level Threats

Persistence		
P1	T1078.001: Valid Accounts: Default Account	Adversaries may obtain and abuse credentials of a default account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Default accounts are those that are built-into an OS, such as the Guest or Administrator accounts on Windows systems.
	T1078.002: Domain Accounts	Adversaries may obtain and abuse credentials of a domain account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Domain accounts are those managed by Active Directory Domain Services where access and permissions are configured across systems and services that are part of that domain. Domain accounts can cover users, administrators, and services.
	T1078.003: Local Accounts	Adversaries may obtain and abuse credentials of a local account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service.
	T1078.004: Cloud Support Accounts	Adversaries may obtain and abuse credentials of a cloud account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application. In some cases, cloud accounts may be federated with traditional identity management system, such as Window Active Directory.
	T1098: Additional Cloud Roles	An adversary may add additional roles or permissions to an adversary-controlled cloud account to maintain persistent access to a tenant.

Mapping Threats to Mitigations

Threat	Mitigation ID	Mitigation	Description
P1	M1032	Multi-factor Authentication	Use two or more pieces of evidence to authenticate to a system; such as username and password in addition to a token from a physical smart card or token generator.
	M1026	Privileged Account Management	Manage the creation, modification, use, and permissions associated to privileged accounts, including SYSTEM and root.
	M1018	User Account Management	Manage the creation, modification, use, and permissions associated to user accounts
	C3.M1	Organization level Authorization Origin Policy	Define actions that are allowed for cloud accounts subscribed to an organization. Ensure policy set to enforce MFA for console and API actions for IAM principles.

Map mitigations to logical controls in OSCAL

```
controls:
  - id: M1032
    class: MITRE Att&ck
    title: Multi-Factor Authentication
    params:
      props:
        - name: label
          value: M1032
          class: MITRE Att&ck
        - name: sort-id
          value: M1032
    links:
      - href: "#M1032"
        rel: required
      - href: "#M1026"
        rel: related
      - href: "#M1018"
        rel: related
      - href: "#C3.M1"
        rel: related
    parts:
      - id: M1032_smt
        name: statement
        prose: "Multi Factor Authentication"
        parts:
          - id: M1032_smt.C3.C1
            name: item
            props:
              - name: label
                value: (C3.C1)
            prose: "Platform must enforce authentication with MFA."
          - id: M1032_smt.C3.C2
            name: item
            props:
              - name: label
                value: (C3.C2)
            prose: " Local authentication must be disabled or restricted."
```

Map mitigations to logical controls in OSCAL

```
- id: M1032_asm-validate
        name: assessment-method
        props:
          - name: method
            value: Validate
            ns: ... #namespace to C3
            class: C3
          - name: label
              value: M1032-Validate
              class: C3
        parts:
          - id: M1032_asm-validate.C3.C1
            name: validate
            props:
              - name: method
                value: (C3.C1)
                class: preventative
            prose: "GIVEN Cloud Platform WHEN principle attempts authentication to perform API action
              THEN platform must enforce multi-factor authentication for each user"
          - id: M1032_asm-validate.C3.C2
              name: validate
              props:
                - name: method
                  value: (C3.C2)
                  class: preventative
            prose: "GIVEN cloud service WHEN principle attempts authentication to the service with
          local credential THEN service should deny action for all principles"
```

Project Workstreams

Define Cloud Services Taxonomy
- CSP agnostic
- Consistent, hierarchical
- Features/Capabilities
- CSP agnostic iconography to represent Services

Engage with MITRE Threat Catalogue
- Identify gaps in the MITRE ATT&CK® framework
- Engage MITRE to extend the framework
- *Start to develop service-specific mitigations*

Engage with NIST on Controls
- Define descriptor language (NIST OSCAL)
- Define a test approach for controls
- *Start to describe logical control(s) per mitigation*

Iterate Common Service Modelling
- Map common CSPs Services to the Services Taxonomy and associated Capabilities
- Model each Common Services
  - identifying Threats and Mitigations
  - Define Logical Controls to represent Mitigations

CSP Certification
- Identify CSP service specific controls to meet Logical Control validators
- Identify CSP specific Test execution framework
- Investigate efficacy of consumer certifications

Citi will seed the first three working groups with initial content and process.

Next Steps: Setting up the Working Groups

- Identify participants for each of the Working Groups:
  - Extending the MITRE ATT&CK! Threat Catalogue
  - Describing Controls with OSCAL
  - Cloud Services Taxonomy

- Agree a meeting cadence and initial co-ordination

- Define initial success criteria, e.g. ~3 months, one common service modelled with:
  - Service taxonomy defined,
  - Threats identified from the MITRE ATT&CK! Framework, gaps identified and extensions modelled,
  - For each threat, controls described using OSCAL

citi

Appendix

Supporting Material

Financial Services Common Cloud Controls – What is it?

The *Financial Services Common Cloud Controls (C3)* standard would consist of the following:

1. **Cloud Services Taxonomy** – a consistent taxonomy for *common critical services* provided by a specific CSP to facilitate identification and classification of *similar services* across CSPs

2. **Service Specific Data Flow Diagram** – a high-level data flow of *a generic service*, providing sufficient details to understand *common attack vectors in the service*. This will necessitate the creation of a consistent nomenclature and iconography for cloud services and their dependent components

3. **Threat Catalogue** – a consistent taxonomy of *common threat techniques* – and associated mitigations – that may occur across services exploiting potential weaknesses. The *MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®)* is proposed to be leveraged and extended where necessary

4. **Logical Controls Description** – a logical control that when implemented would provide a mitigation to a specific threat that a service has to address. The *Open Security Controls Assessment Language (OSCAL)* is a machine-readable data format used to define a control policy. This is a NIST standard that is maturing with controls now available to define the NIST 800-153 cloud standard. However, until recently, this has predominantly been the definition of controls and policies *without definition of the test case or implementation* – this needs to be expanded to be included