Managing Azure at Saxo

Jakob Gottlieb Svendsen – Chief Cloud Engineer – Twitter: @JakobGSvendsen – www.jakobsvendsen.com

Agenda

- Intro to SaxoBank and Our Azure Setup
- What & Why? – Do we really need level ‘hard’?
- How we succeed
- Future Improvements

Parental Leave =

Jakob Gottlie

- Chief Cloud E

ical Pr (CC E)

st in 2

ft C & I y

ex nc

ex nc Gl

er up

dk

s ed n

Ella – 3 years

Leo – 8 months

Saxo Bank Azure

- Largest spend
  - ~ 1400-2000 VMs for Dynamic Test Environments
- Other Azure Services
  - Azure SQL Database
  - Azure Data Bricks
  - Azure App Service Environment (ASE)
  - Azure Functions
  - + many more
- Management Groups
  - DTAP
    - Non-Prod (DT)
    - Production
- Subscriptions
  - One or more per environment
- Project level access, per resource group.

What & Why

SAXO BANK

Jakob Gottlieb Svendsen – Chief Cloud Engineer – Twitter: @JakobGSvendsen – www.jakobsvendsen.com

Why ? - Regulations!

- As a global bank we need to comply to many regulations
- Industry standards, such as
  - SOC2(+)
  - Cloud Security Alliance
  - + more
- Local Governments

Why ? – Change Management

- All Prod Changes have to go through CAB.
- CAB – Change Approval Board
  - Meeting every day
  - Representatives from all areas are present
  - Releasers will be invited to explain, if required.

Why ? – Change Management?!

- Classic Change Management
  - Slow paced
  - Lots of control

- Agile Development
  - Fast paced!
  - No control?!

How do we provide at safe environments, while staying agile?

What ? – Cloud Security Framework

Developed and co-created by Microsoft

This framework specifies **WHAT** security controls must be implemented on workloads running on public clouds and **WHEN** these controls must be implemented.

What ? – Cloud Security Framework

Controls in this framework address Confidentiality and Integrity only, except for security controls that mitigate attacks on service availability (e.g. DDoS protection), with Availability and Recovery requirements being part of the platform or workload design.

What ? – Cloud Security Framework

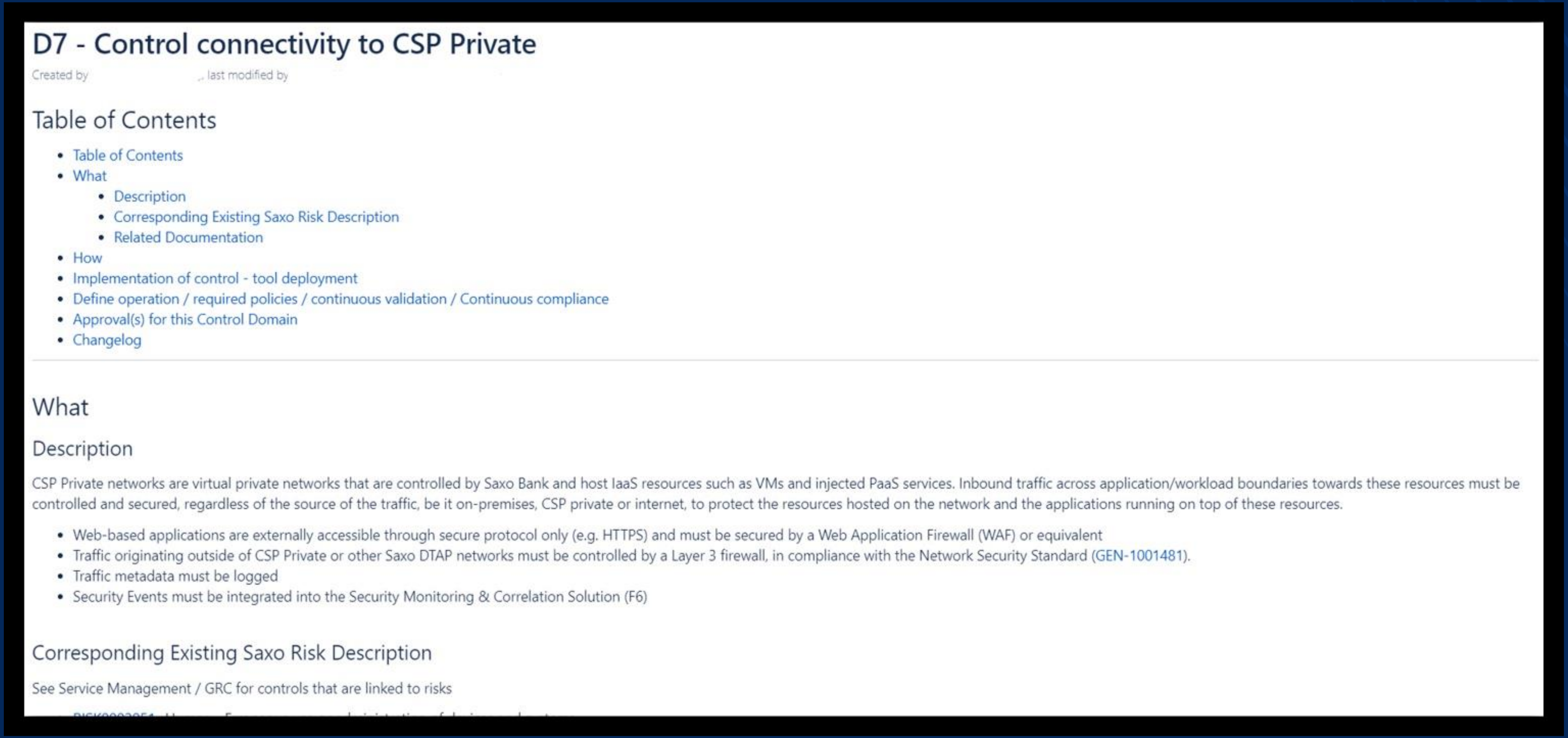
This framework is Cloud Service Provider agnostic.

To give a concrete example of translating **WHAT** to **HOW** and to put a functional description into Azure context, some control slides can have additional Azure specific notes.

When ? – Cloud Security Framework

- **Playground**
  - Non-production/private connected workloads
- **Standard**
  - Default container for all production workloads (it is expected that approx. 80% fits into this category)
- **Advanced**
  - Container for workloads/data with high confidentiality and criticality
- Based on Group Information Classification Policy (POL-1002509), including Personal Data Classification Policy (POL-1002500)

Example – Cloud Security Framework



D7 - Control connectivity to CSP Private

Created by , last modified by

Table of Contents

What

Description

CSP Private networks are virtual private networks that are controlled by Saxo Bank and host IaaS resources such as VMs and injected PaaS services. Inbound traffic across application/workload boundaries towards these resources must be controlled and secured, regardless of the source of the traffic, be it on-premises, CSP private or internet, to protect the resources hosted on the network and the applications running on top of these resources.

- Web-based applications are externally accessible through secure protocol only (e.g. HTTPS) and must be secured by a Web Application Firewall (WAF) or equivalent
- Traffic originating outside of CSP Private or other Saxo DTAP networks must be controlled by a Layer 3 firewall, in compliance with the Network Security Standard (GEN-1001481).
- Traffic metadata must be logged
- Security Events must be integrated into the Security Monitoring & Correlation Solution (F6)

Corresponding Existing Saxo Risk Description

See Service Management / GRC for controls that are linked to risks

How

Security Controls

- Log
  - Log Analytics Workspace(s)
- Policies
  - Tags
  - Connectivity (Block public IP use)
- Runbooks
  - Audit
    - Collect to Log Analytics
      - Built in – Azure Diag Logs, Audit Logs
      - Custom
  - Modify
    - Set Azure Diag Logs etc.
    - Groom Permissions
- Alerts
  - Defined in an excel sheet for audit purposes
  - Auto generated into json, then deployed via pipeline

Azure Service Certification

- A process to make sure that no Azure solutions are implemented using azure services or settings that are not allowed by Global Information and Cyber Security (GICS).
- This ensure the compliant use of services.
  - What services can be used
  - What configurations are allowed.
- Examples:
  - We can enforce encryption of data at rest or in motion even for services, where it is optional.
- It facilitates a central template repository.

Benefits of Service certification

- **Developers:**
- It provides central repository which is easy to access.
- No redundancy of code.
- Saves development efforts and time.
- Security compliant services.
- No worries for updates in services, it also allows central updates of configuration. i.e.
  - Windows OS image to be used (max 30 days old)

- **Management:**
  - Standard use of services across the Saxo.
  - Easy maintenance due to central repository.
  - Minimize risk for misuse of services.
  - Rightsizing SKUs
  - It also save development cost by saving development time.

How to get your service certified

- **The development team is responsible for creating**:
- **Create ARM template for the service**
- **Create sample JSON for test deployment**
- **Create Readme.md for service template**
- Raise pull request for Cloud Foundation and security team.
- **Cloud Foundation team is responsible for** :
- Review templates and readme documents in pull request.
- Sign and approve your pull request.
- After getting approval from CF team create separate pull request for GICS team.
- **GICS team responsibility**:
- GICS team will review this from security point of view.
- Sign and approve your pull request.
- Finally, service owner approval.

Cloud Application CI

- ServiceNow Configuration Item
- Business Service
- Owner
- Budget
- Data & Use - Classification
- Support

Demo – Cloud App

DevOps Tasks

- Custom DevOps Tasks Actions
  - Create/Update Resource Group
  - Approved PowerShell Scripts
  - Azure AD App Registrations
  - Deploy SQL Database
  - SQL Identity / Access
  - Package Deployer (Code to VM)
  - + More

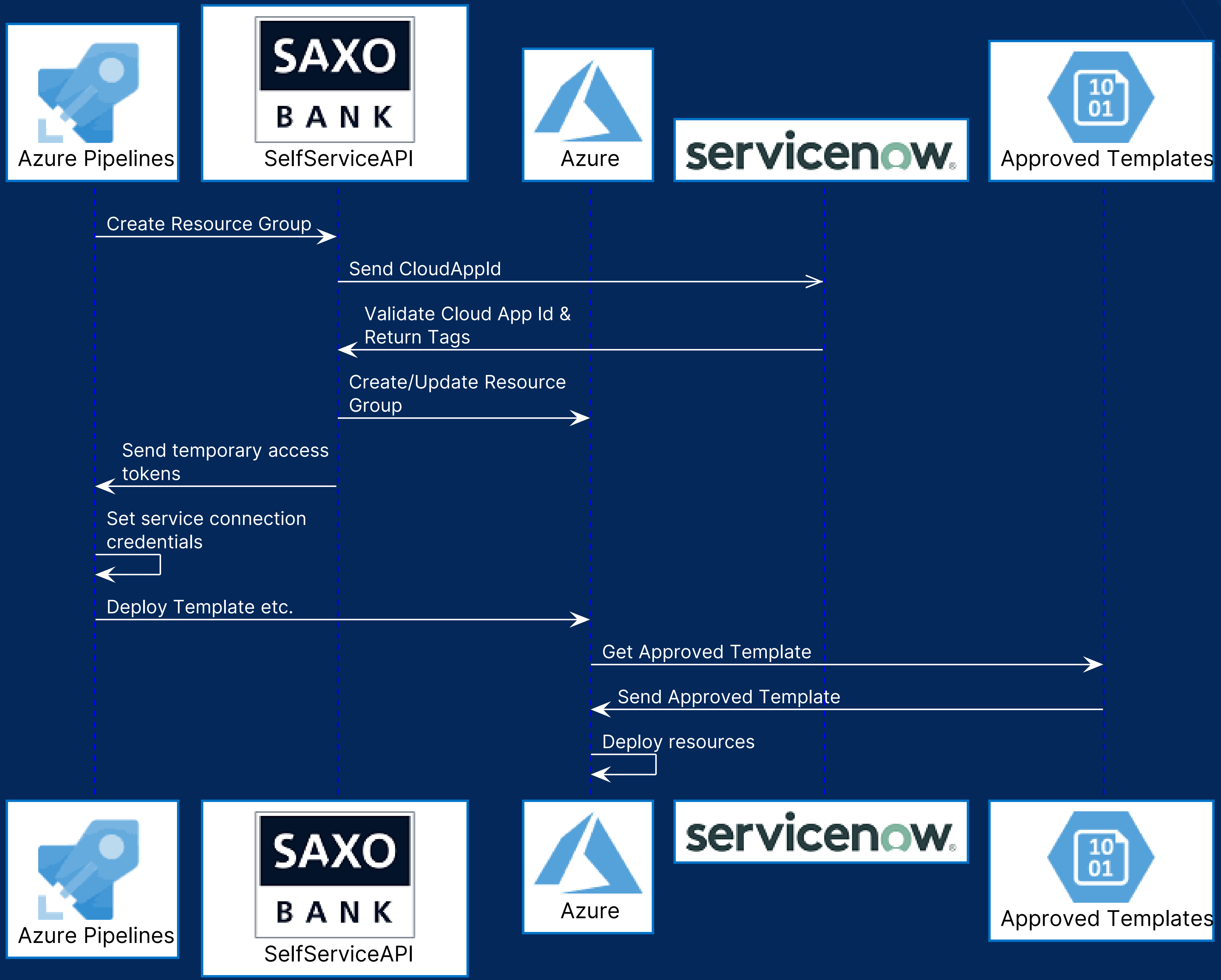
DevOps Tasks

- Allowed Tasks
  - Saxo DevOps Deploy Tasks (Deploy package etc.)
  - Saxo Cloud Tasks (Create RG etc.)
  - Saxo Change Tasks (Create Change etc.)
  - Saxo Bank Rotate Keys
  - Azure App Service Deploy
  - Azure App Service Manage
  - Azure Resource Group Deployment
  - AzureBlob File Copy
  - Databricks
    - Create Bearer Token
    - Deploy Cluster
    - Deploy Notebooks
    - Deploy Secret
    - files to DBFS
  - **PowerShell Script**
  - Visual Studio Test

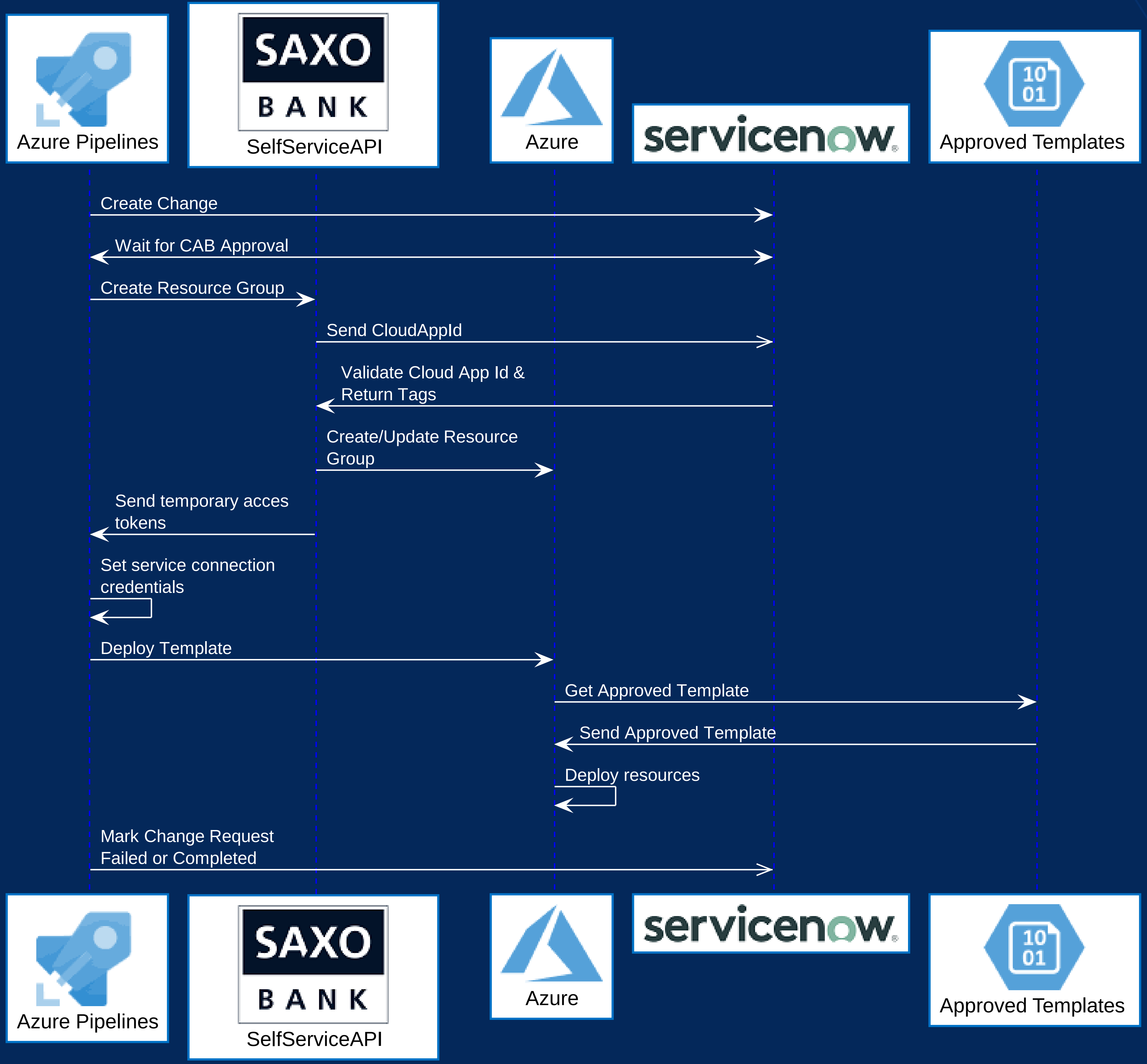
Create Resource Group

- A gate to apply rules
- Enable temporary access in the same stage
- Checks
  - Tasks used
  - Template - Azure Resources used
  - Production - Change Request is in progress
  - Production – only master branch from approved templates
- Special rules for certain projects (only development)

Create Resource Group Flow



Production Release



Create Change

Wait for CAB Approval

Create Resource Group

Send CloudAppId

Validate Cloud App Id & Return Tags

Create/Update Resource Group

Send temporary acces tokens

Set service connection credentials

Deploy Template

Get Approved Template

Send Approved Template

Deploy resources

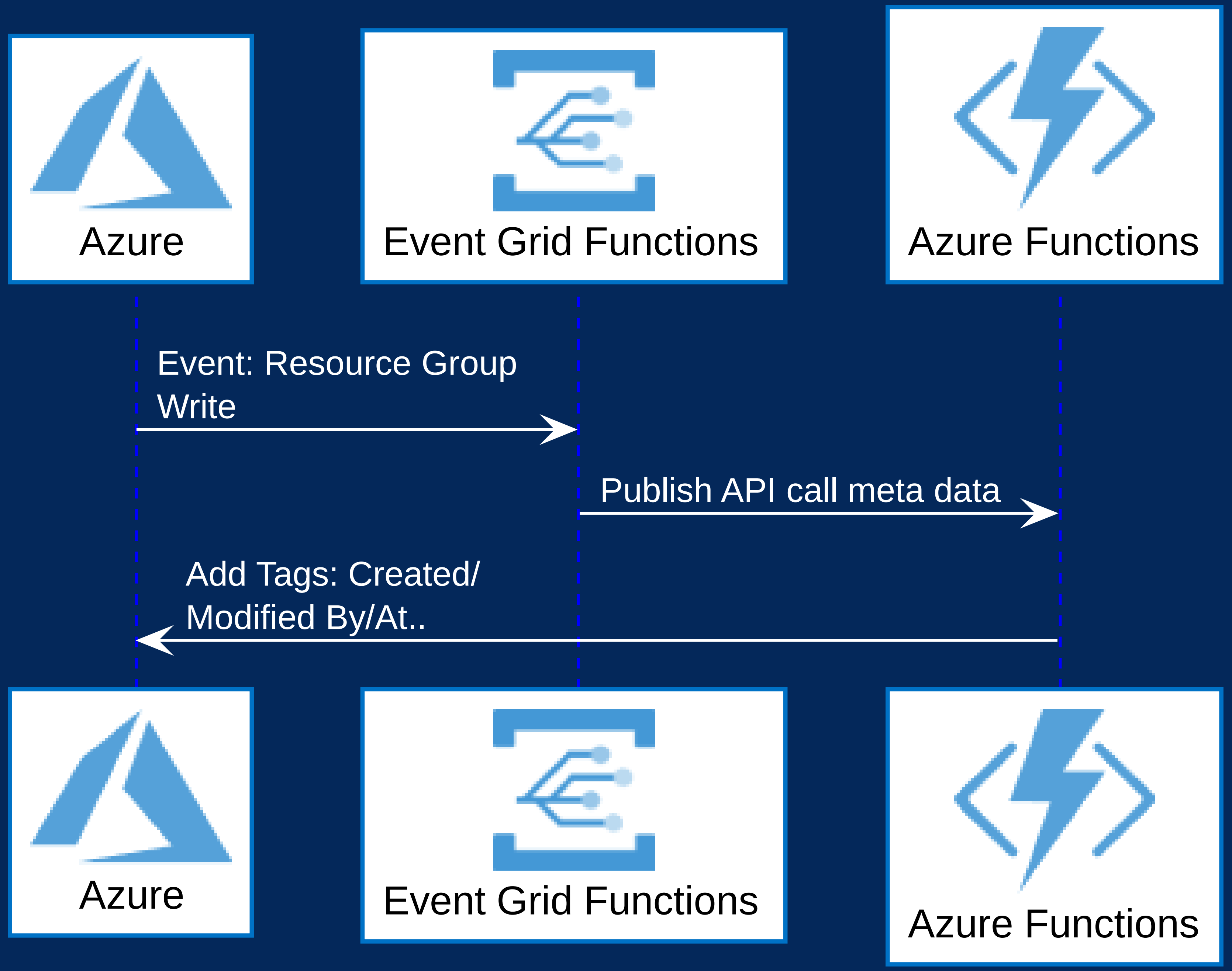
Mark Change Request Failed or Completed

Demo - Pipeline

Low Risk Cab

- Follow a set of rules
  - Development methods
  - Automated Testing
  - Smoke Tests
  - Automated and Tested Rollback
  - + more
- Allowed deployment without manual approval from CAB
- Create Change Task Support it

Add Meta Tags


Azure
Event Grid Functions
Azure Functions
Event: Resource Group Write
Publish API call meta data
Add Tags: Created/ Modified By/At..
Azure
Event Grid Functions
Azure Functions

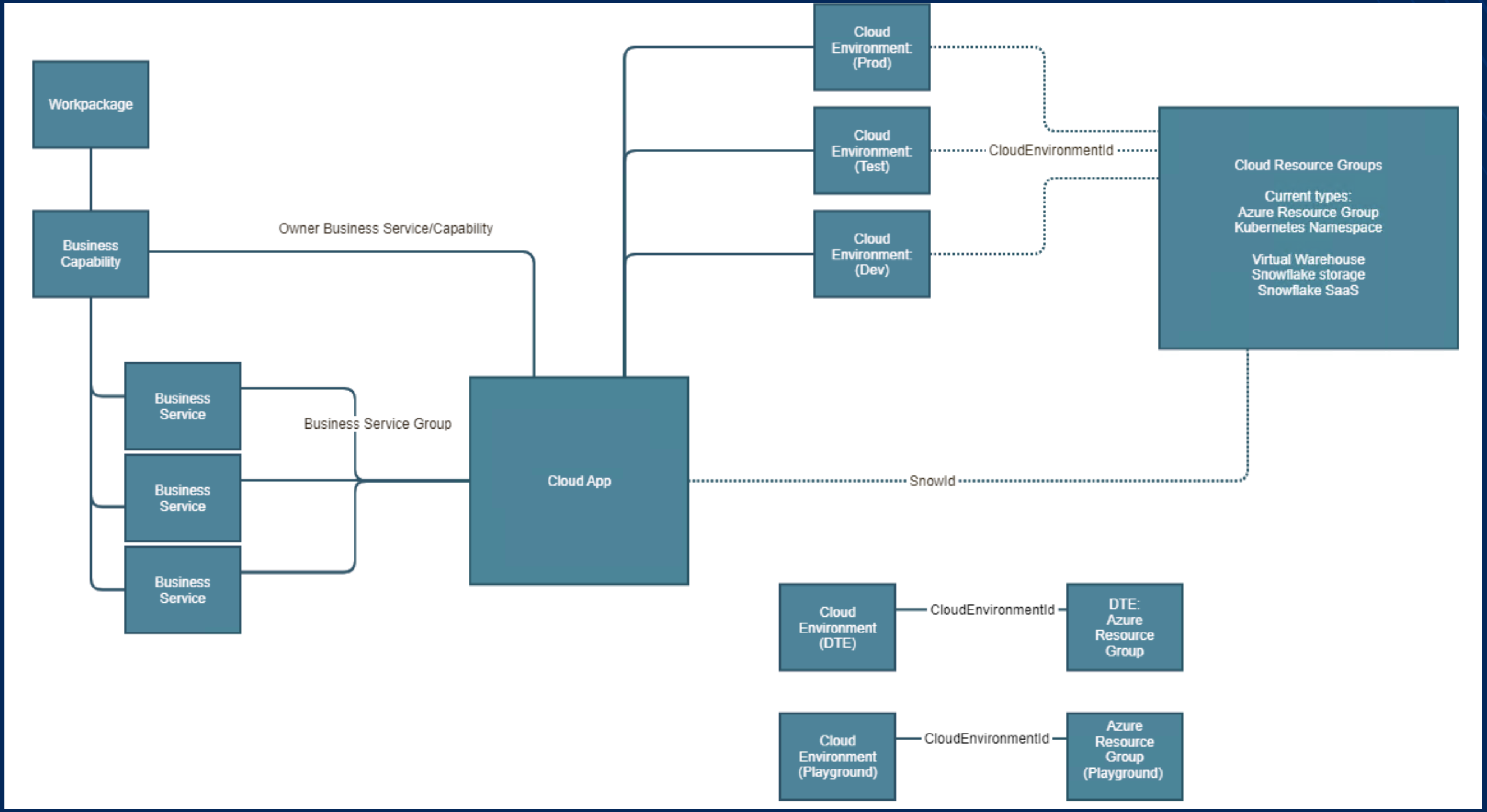
Demo – Event Based Tags

New / Future

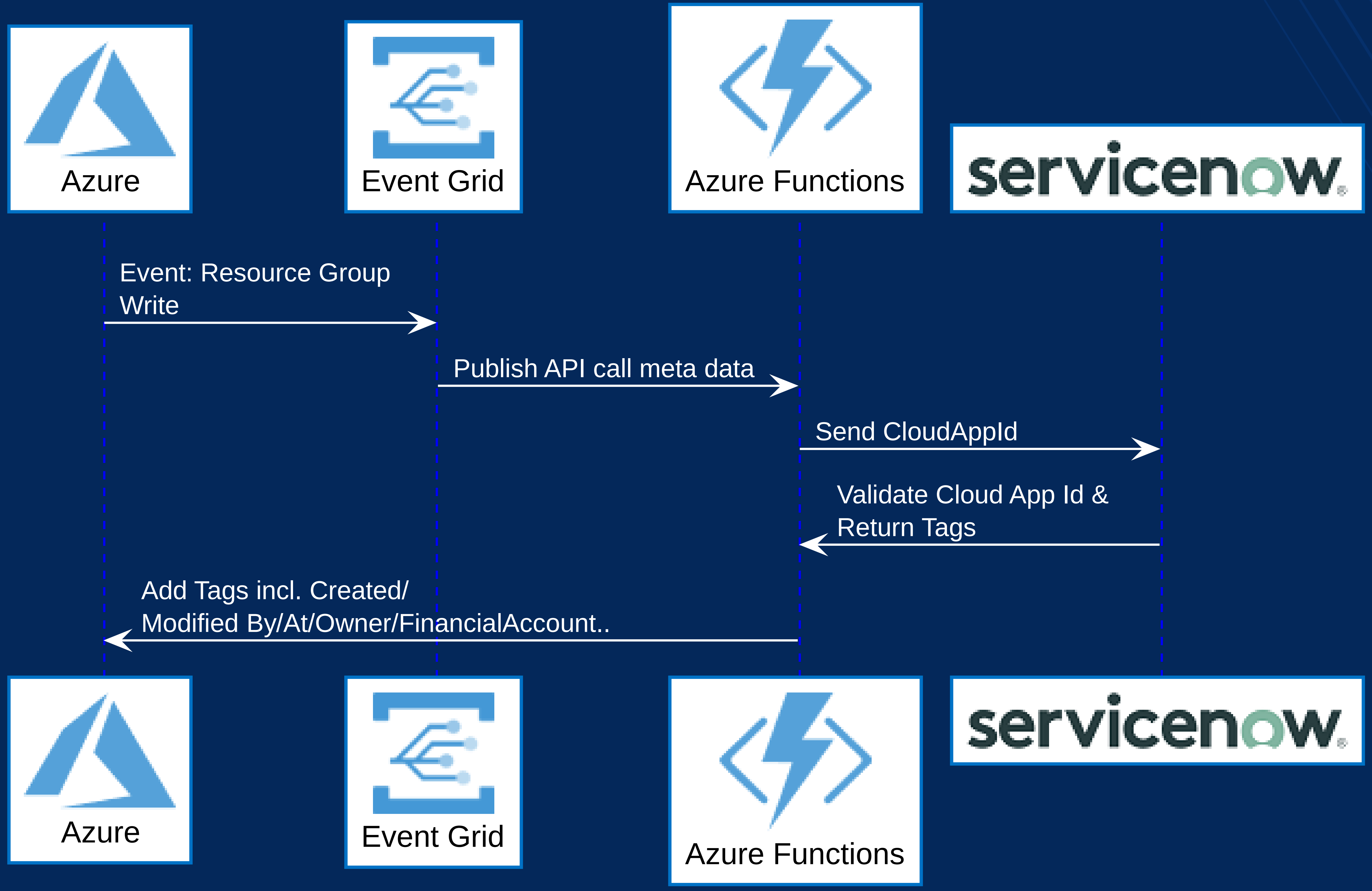
Cloud Environment CI

- Child of Cloud App
- Auto Returned from ServiceNow Based on environment
- Provides option to split reports by environments
  - Development
  - Test
  - Acceptance
  - Production

New Cost Management Architecture



Add Meta Tags – With Service Now


Azure
Event Grid
Azure Functions
servicenow
Event: Resource Group Write
Publish API call meta data
Send CloudAppId
Validate Cloud App Id & Return Tags
Add Tags incl. Created/ Modified By/At/Owner/FinancialAccount..
Azure
Event Grid
Azure Functions
servicenow

Management Groups (Work in Progress)

- CSP Private - Connected
  - DTAP
    - DT
      - Development
      - Test
    - Production
- CSP Public – Isolated
  - DTAP
    - DT
      - Development
      - Test
    - Production
  - Playground

New Reference architecture

- In use in production already
  - (Azure) Kubernetes
  - Elastic Search
  - Kafka
  - Kibana
  - + more
- Security Framework controlled by k8s policies
- Internal package/image source (Jfrog)

Questions?

- Today: Q & A at 1745 – 1815
- JakobGSvendsen
  - Twitter
  - LinkedIn
  - GitHub
  - Powershellgallery.com

www.jakobsvendsen.com