

One Platform Country Hosting   
TID Template - Lite

Ver 2.0

# Introduction

The Purpose of this document is to provide high level details of the proposed solution implementation and deployment. This document will give Security and ITS Platform team a general understanding of the application and will be used as a reference point for initial conversations, objective is to start the endorsement process and allow business units to progress developing the end solution in Dev/Sandbox subscriptions.

# Project Information and Solution Design

This section provides a detailed introduction of the project and a high-level overview of the solution architecture. Prior to completing this template its strongly advised to research the [Global Enterprise Architecture Portal](https://ea-reports.kworld.kpmg.com/apm/powerbi/Portfolio%20Reports/Enterprise%20Portfolio?rs:Command=Render&rc:Toolbar=false) for a capability match. Please contact the Technical Manager (Nicola Duncan) for EA for more information.

## 

## Project Name and Description

### Project name: ACC Claim Portal

### Sponsoring partner: Adam McManus

### Application owner: Han Li

### Application name: ACCCP

### Broad functionalities provide by application (This helps ITS understand context)

### Project Start Date: 09/09/24

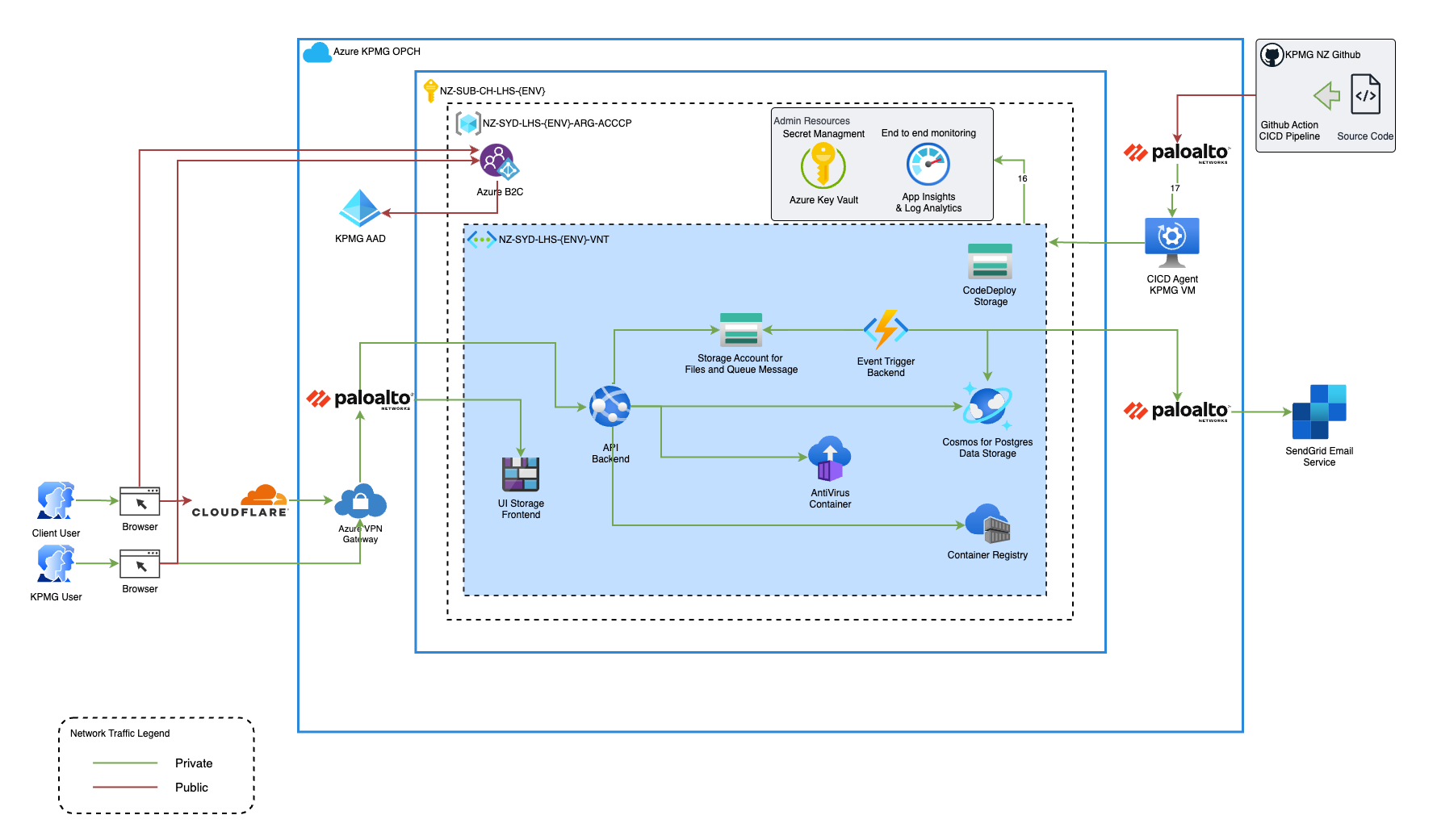
### Project Go-Live / End Date: 09/10/24 / TBC

## Solution Information

|  |  |
| --- | --- |
| Solution & Components Information | |
| **Item** | **Response** |
| Azure Location | AU East |
| Environment – (Prod, Dev, QA or Staging) | Dev |
| Has the proposed design been used previously | Yes |
| Resources Required (IaaS, PaaS, Storage) | Storage Account, Function App, App Service, Container App, App Insight, Key Vault, B2C, Cosmos DB, Container Registry |
| Is there a 3rd party Vendor involved | SendGrid |
| Does application require Client authentication | Yes, through B2C for client |

# Architecture Core Design

Supply a HL visual Diagram of the application.



With reference to the supplied architecture above, each component needs to be explained with a view to ensure components sit within our security boundaries. Pre-approved Azure PaaS components are Private Link capable to run within our private network. Secure gateways are already established, Cloudflare, VM-Series and Application Gateway for ease of deployment.

**Ports required.**

* Ingress 5432 and 6432 on cosmosdb
* Ingress 3310 on antivirus container
* Egress 5432, 6432, 3310 on Api App Service and Event Trigger Backend Function App

**Describe the Traffic Flow [Example]**

* Internal KPMG User login via SSO with B2C integrated with KPMG AAD
* External User login via SSO or Email Password with B2C
* User’s traffic will pass through KPMG Cloudflare, to VPN Gateway, through Paloalto, then to static UI storage account.
* User’s traffic will pass through KPMG Cloudflare, to VPN Gateway, through Paloalto, then to API Service resources.
* API services will communicate with Cosmos, File Storage Account and AntiVirus Container for any user action.
* Github Action traffic will pass through Paloalto, KPMG Github CICD Agent, then to container registry.
* Function App will send request to Sendgrid passing through Paloalto.
* All resource sends logs to application insight.

# Azure Resource Baseline Configuration Standards

Wherever possible, all internet facing systems in KPMG NZ OPCH need to be configured to go through: Cloudflare → Azure External Load Balancer → Palo Alto Firewall → Application Gateway (optional) → IaaS resource interface or private endpoints of PaaS services.

## IaaS VM Operating Systems

## Whenever possible, use Azure PaaS service instead of Azure IaaS virtual machine to be as internet facing systems. All the IaaS VMs must be hardened as per global standard to reduce the attack surface [Security Standard - Server Virtualization.pdf (kpmg.com)](https://spo-global.kpmg.com/sites/kz-oi-bus-QRM/Shared%20Documents/iss/Standards/Security%20Standard%20-%20Server%20Virtualization.pdf).

## For domain joined Windows servers, they should be put in correct organization unit so that the global standard group policy objects can secure them to meet the security requirements. The Windows Server group policies are applied at KPMG NZ domain from the following Organization Unit OU=Servers,DC=nz,DC=kworld,DC=kpmg,DC=com so the Windows Servers will need to be put in the proper sub OU(s).

## Also make sure the other KPMG NZ virtual server management and monitoring tools (SCCM, GPO, MS Defender, Crowdstrike, PRTG etc.) are installed and configured properly.

## Non domain joined Windows servers must be built from the customized server image with the global security standards <https://spo-global.kpmg.com/sites/GO-OI-BUS-GTK/OnePlatform/IT-StandardWindowsServer2022.pdf> with those KPMG NZ virtual server management and monitoring tools when possible.

## If the internet facing system must run in Linux, Red Hat Enterprise Linux 8 is the global standard Linux operating system, and they need to be setup and configured according to global standard.

I:\General\IT\Standards\IT Standard - RedHat Enterprise Linux8 v1.0.pdf

## PaaS Services

### Identity and Access Management

* Configure the least RBAC role to those who need to access theses PaaS services.
* Use Azure Managed Identities to securely authenticate PaaS services to other Azure services without storing credentials.
* Whenever possible, Use Azure AD for identity management, authentication, and authorization. Implement multi-factor authentication (MFA) for added security (enforced by the global already).

### Network Separation and Security

* User virtual networks and subnets to isolate PaaS services from the public internet and other resources and implement Network Security Groups (NSGs) to control traffic follow.
* Whenever possible use Azure Private Endpoints to access PaaS services privately from within KPMG virtual network.
* All the traffic between virtual networks, and to and from On-premises network need to be inspected by OPC Palo Alto firewall.
* Disable the provision of public interface via Azure firewall.

### Data Security

* Encryption at Rest: Enable encryption at rest for Azure Storage accounts, Azure SQL Databases, and other data services.
* TLS/SSL: Use Transport Layer Security (TLS) or Secure Sockets Layer (SSL) to encrypt data in transit for web applications and APIs.
* Data Classification: Classify and label sensitive data and implement data loss prevention (DLP) policies using Azure Information Protection.
* Database Security: Apply database-level encryption, auditing, and role-based access control for Azure SQL Databases.

### Monitoring and Logging

* Azure Monitor: Set up Azure Monitor to collect telemetry data from PaaS services. Create alerts and use Azure Monitor Logs for advanced analytics.
* Azure Security Centre: Enable Azure Security Centre to monitor security configurations, detect threats, and provide security recommendations.
* Logging: Configure centralized logging using Azure Monitor Logs and Azure Application Insights to gain insights into application and infrastructure performance and security.

### Container Security

* Azure Kubernetes Service (AKS): If using AKS, follow container security best practices, including regular vulnerability scanning, image signing, and RBAC.
* Container Registry: Use Azure Container Registry for secure image storage and distribution. Implement image scanning for vulnerabilities.

### Technical Standards

[Technology Standards (kpmg.com)](https://spo-global.kpmg.com/sites/GO-KPMG_Technology_Standards). Technology Standards are a collection of requirements that relate how a product will be implemented throughout KPMG. All published Technology Standards are mandatory throughout the KPMG network of member firms.

The Global Technical Standards have been reviewed and it is confirmed that non are applicable for this deployment.

**OR**

The Global Technical Standard have been reviewed and the following standards are applicable to this deployment, and will be configured in line with the standard accordingly:

* Link to first standard
* Additional link as applicable

Note that non-compliance to Global Technology Standards must be raised as an exemption request for global sign off. If required, please email [InfoSec@kpmg.co.nz](mailto:InfoSec@kpmg.co.nz).