**CORE SERVICE DESIGN:**

**Azure App Gateway**

atabricks

|  |  |
| --- | --- |
| IT Owner Details | |
| **Department** | DTS |
| **Contact Name** | Dominic Panzera |
| **Address** | 375 Manningham Road, Doncaster, Victoria 3108 |

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Azure App Gateway Core Service Design |
| **File Name** | Ambulance Victoria – Azure App Gateway Core Service Design v1.0.docx |
| **Version** | 1.0 |
| **Status** | Released |
| **Release Date** | 8/03/2024 |

|  |  |  |  |
| --- | --- | --- | --- |
| Preparation |  |  |  |
| **Prepared** | Daniela Nikolic |  |  |
| **Authorised** | Dileep Pradeep |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 8/03/2024 |

Table of Contents

[1. Overview 5](#_Toc160613907)

[1.1 Purpose and Audience 5](#_Toc160613908)

[1.2 Scope and Key Deliverables 5](#_Toc160613909)

[1.3 Glossary and Definitions 6](#_Toc160613910)

[2. Executive Summary 7](#_Toc160613911)

[3. Resource Cost 8](#_Toc160613912)

[4. WAF and Security Control Alignment 8](#_Toc160613913)

[4.1 Reliability 9](#_Toc160613914)

[4.1.1 Overview 9](#_Toc160613915)

[4.1.2 Azure App Gateway Reliability Checklist 9](#_Toc160613916)

[4.2 Cost Optimisation 10](#_Toc160613917)

[4.2.1 Overview 10](#_Toc160613918)

[4.2.2 Azure App Gateway Cost Optimisation Checklist 10](#_Toc160613919)

[4.3 Operational Excellence 11](#_Toc160613920)

[4.3.1 Overview 11](#_Toc160613921)

[4.3.2 Azure App Gateway Operational Excellence Checklist 11](#_Toc160613922)

[4.4 Performance Efficiency 12](#_Toc160613923)

[4.4.1 Overview 12](#_Toc160613924)

[4.4.2 Azure App Gateway Performance Efficiency Checklist 12](#_Toc160613925)

[4.5 Security 13](#_Toc160613926)

[4.5.1 Overview 13](#_Toc160613927)

[5. Architecture Summary 14](#_Toc160613928)

[5.1 Resource Overview 14](#_Toc160613929)

[5.1.1 Networking Requirements 14](#_Toc160613930)

[5.2 RBAC 14](#_Toc160613931)

[5.3 Design Decisions and Justifications 15](#_Toc160613932)

[5.3.1 Version 15](#_Toc160613933)

[5.3.2 WAF 15](#_Toc160613934)

[5.3.3 Health Probes 15](#_Toc160613935)

[5.3.4 Scaling 16](#_Toc160613936)

[5.3.5 Monitoring 16](#_Toc160613937)

[5.3.6 Logging 16](#_Toc160613938)

[5.3.7 Instance Counts 16](#_Toc160613939)

[5.3.8 Networking 17](#_Toc160613940)

[5.3.9 Secrets and Credentials 17](#_Toc160613941)

[5.3.10 Encryption 17](#_Toc160613942)

[6. Azure Policies 17](#_Toc160613943)

[7. Configuration Templates 18](#_Toc160613944)

[7.1 Primary Production Application Gateway 18](#_Toc160613945)

[7.2 Secondary DR Application Gateway 19](#_Toc160613946)

[7.3 Primary Non-Production Application Gateway 20](#_Toc160613947)

[8. Acceptance 21](#_Toc160613948)

# Overview

This document covers the baseline design for the Azure App Gateway core service. The intention of this document is to define the overall resource design in isolation from a specific application. It is aimed to highlight the general process and requirements for building a Azure App Gateway in a repeatable fashion with consistent configurations. Design decisions and justifications have been included in the Architecture section, and this document can be used as a reference for new builds that require a Azure App Gateway.

This design caters to a Level 2 design which covers both Microsoft’s WAF (Well Architected Framework)[[1]](#footnote-2) and the Department of Health Control list.

Any deviations required to the standards defined in this document will require separate exemption and approval from the Cloud Governance Forum if they are required for any reason for a specific build.

## Purpose and Audience

This document will outline the standard design and configuration of this Azure service in Ambulance Victoria’s Azure tenancy as a baseline for any application infrastructure deployments.

This design is intended to:

* Meet Microsoft WAF standards.
* Meet the controls stipulated by the Department of Health.
* Define the baseline required for the deployment of the resource.

The audience for this document is those involved in the planning, designing, and implementing of the Application/Data infrastructure. This includes:

* + Ambulance Victoria IT staff

It is assumed that the reader knows and is familiar with Azure Cloud concepts and related topics.

## Scope and Key Deliverables

The scope of this core service design is to define the baseline deployment requirements and standards for the Azure App Gateway core service.

The key deliverables for this are:

* This design to outline the service definition Level 2 baseline standards.
* A technical configuration document that defines the deployment of this resource for each of the Service Tiers, or for any other logical standard such as size
* IaC templates for repeatable deployment of this core service

## Glossary and Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **AV** | Ambulance Victoria |
| **WAF** | Well Architected Framework |
| **CAF** | Cloud Adoption Framework |
| **Level 1** | Refers to a resource that has been designed to a CAF standard |
| **Level 2** | Refers to a resource that has been designed to a WAF standard with Department of Health controls overlayed |
| **AZ 2** | Refers to Ambulance Victoria’s legacy Azure Landing Zone still in use in some regards |
| **AZ 3** | Refers to Ambulance Victoria’s current Azure Landing Zone, also referred to as the Enterprise landing zone. This is the target state for migrations. |
| **SLA** | Service Level Agreement as defined by Microsoft |
| **DH** | Department of Health |
| **IaC** | Infrastructure as Code |
| **NSG** | Network Security Groups |

Table 1: Glossary and definitions

# Executive Summary

This design covers the baseline standards for the Azure App Gateway Core Service. This service has been assessed against the five pillars of WAF as well as the Department of Health Security Controls.

This section contains a summary of the major design decisions that have been made for defining the baseline of this resource as an outcome of the WAF and Security analysis detailed throughout this document.

Of the five WAF Pillars, it was found that Reliability, Performance Efficiency, Operational Excellence, Cost Optimisation and Security were relevant.

For this service the main baseline configurations include:

* Azure App Gateway WAF V2 will be used
* A network with a minimum of /26 is required to be dedicated to App Gateway
* An exception for the Route Table standard deployments will be required.
* Health probes will be used
* NetworkWatcher will be used for Network Insights
* Key Vault will be used to store any associated certificates

There are some minor differences between Production and Non-Production deployments:

* Autoscaling will be enabled for Production, and will not be enabled for Non-Production
* A minimum instance count of 2 and maximum of 10 will be used as the defaults for Production

# Resource Cost

The following is the resource cost for Azure App Gateway, it assumes V2 is in use[[2]](#footnote-3):

|  |  |  |
| --- | --- | --- |
| Not available | Application Gateway | Web Application Firewall Application Gateway |
| Fixed | **$0.4278** per gateway-hour | **$0.7699** per gateway-hour |
| Capacity Unit1 | **$0.0123** per capacity unit-hour | **$0.0220** per capacity unit-hour |

Table 2: Pricing construct

# WAF and Security Control Alignment

The following are the five pillars of the Microsoft Well Architected Framework:

* [Reliability](https://learn.microsoft.com/en-us/azure/well-architected/#reliability)
* [Cost optimization](https://learn.microsoft.com/en-us/azure/well-architected/#cost-optimization)
* [Operational excellence](https://learn.microsoft.com/en-us/azure/well-architected/#operational-excellence)
* [Performance efficiency](https://learn.microsoft.com/en-us/azure/well-architected/#performance-efficiency)
* [Security](https://learn.microsoft.com/en-us/azure/well-architected/#security)

For this design, the security section will also cover the Department of Health Controls in addition with any Microsoft Security Best Practices. Each of these sections will detail relevant controls or baseline requirements for this core service that will be put in place.

## Reliability

### Overview

The term reliability refers to the availability of the system and its ability to recover from failure[[3]](#footnote-4). Resiliency strategies must be built into each element of the architecture. The pillars of reliability include:

* Design for business requirements
* Design for failure
* Observe application health
* Drive Automation

### Azure App Gateway Reliability Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **R1** | Plan for rule updates | Yes | No | Governance | Operational |
| **R2** | Use health probes to detect backend unavailability | Yes | No | IaC | Operational – during application design specific endpoints can be added to the IaC |
| **R3** | Review the impact of the interval and threshold settings on health probes | Yes | No | Governance | Operational – during application design |
| **R4** | Verify downstream dependencies through health endpoints | Yes | No | Governance | Operational – during application design and deployment |
| **R5** | When using Azure Front Door and Application Gateway to protect HTTP/s applications, use WAF policies in Front Door and lock down Application Gateway to receive traffic only from Azure Front Door. | No - Front Door not allowed by Security | No | N/A | N/A |

Table 3: WAF Reliability checklist summary

## Cost Optimisation

### Overview

The cost optimisation pillar is structured to support creating cost-effective workloads in the cloud[[4]](#footnote-5). It looks at removal of unnecessary spend and improving operational efficiency. The principles of cost optimisation revolve around:

* Choosing the correct resources
* Setting up budgets and maintaining cost constraints
* Dynamically allocate and deallocate resources
* Optimising workloads whilst aiming for scalable costs
* Continuously monitoring and cost managing

### Azure App Gateway Cost Optimisation Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **CO1** | Familiarize yourself with Application Gateway pricing | Yes | No | Governance | Operational |
| **CO2** | Review underutilized resources | Yes | No | Governance | Operational – during deployment |
| **CO3** | Stop Application Gateway instances when not in use | Yes | No | Governance | Operational – for non-prod deployments |
| **CO4** | Have a scale-in and scale-out policy | Yes | Yes | IaC | At deployment |
| **CO5** | Review consumption metrics across different parameters | Yes | No | Governance | Operational – during deployment |

Table 4: WAF Cost Optimisation checklist summary

## Operational Excellence

### Overview

Operational Excellence aims to ensure that once the architecture is built, the ongoing operations are flawless. This includes repeatable and reliable deployments, automating to eliminate human error. To do this the following must be considered:

* Optimise the build and release process (including CI/CD and IaC)
* Understand Operational Health
* Test recovery and failure
* Focus on continuous improvement
* Use loosely coupled architecture

### Azure App Gateway Operational Excellence Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **OE1** | Monitor capacity metrics | Yes | Yes | IaC – Diagnostic settings | At deployment |
| **OE2** | Troubleshoot using metrics | Yes | No | Governance | Operational – during deployment |
| **OE3** | Enable diagnostics on Application Gateway and Web Application Firewall (WAF) | Yes | Yes | IaC | At deployment |
| **OE4** | Use Azure Monitor Network Insights | Yes | No | IaC – NetworkWatcher | At deployment |
| **OE5** | Match timeout settings with the backend application | Yes | No | Governance | Operational – during application design and deployment |
| **OE6** | Monitor Key Vault configuration issues using Azure Advisor | Yes | No | Governance | Operational – during deployment |
| **OE7** | Consider SNAT port limitations in your design | Yes | No | Governance | Operational – during application design |

Table 5: WAF Operational Excellence checklist summary

## Performance Efficiency

### Overview

Performance Efficiency refers to the ability of your systems and applications to meet user demands without breaking or creating a negative user experience[[5]](#footnote-6). This covers capacity and scalability:

* Design for horizontal scaling
* Run stress and performance tests
* Continuously monitor performances, particularly in Production systems

### Azure App Gateway Performance Efficiency Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **PE1** | Estimate the Application Gateway instance count | Yes | No | Governance | Operational – during application design |
| **PE2** | Define the minimum instance count | Yes | Yes | IaC | At deployment |
| **PE3** | Define the maximum instance count | Yes | Yes | IaC | At deployment |
| **PE4** | Define Application Gateway subnet size | Yes | Yes | IaC – Virtual Network | At deployment |
| **PE5** | Take advantage of features for autoscaling and performance benefits | Yes | Yes | IaC | At deployment |

Table 6: WAF Performance Efficiency checklist summary

## Security

### Overview

Security refers to the ability of the environment to resist and manage threats.

This section covers both Microsoft Best Practices as well as relevant security controls provided by the Department of Health. With respect to the Microsoft WAF, Security is underpinned by the following[[6]](#footnote-7):

* Plan resources and how to harden them
* Automate and use least privilege
* Classify and encrypt data
* Monitor system security, plan incident response
* Identify and protect endpoints
* Protect against code-level vulnerabilities
* Model and test against potential threats

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The following Microsoft Security Benchmark controls are applicable:

* NS-1: Establish network segmentation boundaries
* NS-2: Secure cloud services with network controls
* IM-8: Restrict the exposure of credential and secrets
* DP-3: Encrypt sensitive data in transit
* DP-7: Use a secure certificate management process
* LT-4: Enable logging for security investigation

# Architecture Summary

## Resource Overview

Azure Application Gateway is a load balancer for web traffic (OSI layer 7)[[7]](#footnote-8). It is used for load balancing traffic to web applications, unlike the Azure Load Balancer which sits at Layer 4 OSI and balances TCP and UDP traffic. It also has capability to perform:

* SSL/TLS termination
* WAF (Web Application Firewall) functions

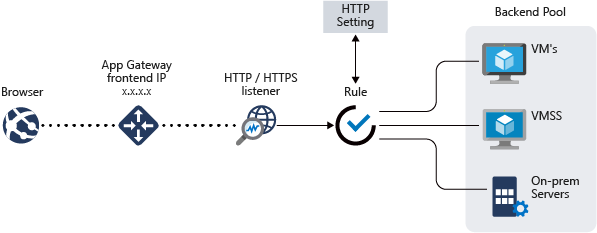


Figure 1: Web traffic balancing with Azure App Gateway[[8]](#footnote-9)

The Application Gateway can be deployed in spokes, or centrally as is the case with the current deployment in the Perimeter Services landing zone.

### Networking Requirements

An App Gateway requires a dedicated subnet, though multiple instances of the Gateway can be within the same subnet[[9]](#footnote-10). A subnet of /24 is typically recommended to allow for scale out and future growth, however the minimum recommended is /26. s

## RBAC

For the Azure Application resource, the specific roles that can be applied are as follows:

|  |  |
| --- | --- |
| Role Name | Description |
| Network Contributor | Lets you manage networks, but not access to them. |

Table 8: RBAC roles relevant for this core service

## Design Decisions and Justifications

This section covers the design decisions and justifications that reflect the findings of the WAF and Security alignment. This will form the baseline requirements for the Azure App Gateway core service and will be captured in the accompanying Configuration Template with a set of pre-approved deployment settings for this resource. Any changes, modifications or removals to the pre-approved deployments must have specific approval from the Cloud Governance Forum prior to deployment.

### Version

**Design Reference:** N/A

**Design Decision:** App Gateway WAF V2 SKU will be used.

**Design Justification**: WAF V2 offers significant feature improvements compared to V1 including the ability to integrate with Azure Key Vault, write custom WAF policies, and has connectivity via Private Link as an option.

### WAF

**Design Reference:** N/A

**Design Decision:** The WAF functionality is assumed to be required unless the Gateway is purely being used to load balance web traffic and the traffic is being handled by another Firewall. If not required, the Standard V2 SKU can be used.

**Design Justification:** The WAF functionality is not always required but will be set as a default value. Currently the Perimeter Services landing zone acts as an entry point for web traffic for public facing applications, so this has the WAF functionality enabled to inspect incoming traffic. In other use-cases this feature may not be required.

### Health Probes

**Design Reference:** Table 3 – [R2](#_Azure_App_Gateway)

**Design Decision:** Health probes will be used for backends.

**Design Justification:** Health probes will be enabled as this allows the App Gateway to monitor health of its backends, and it will automatically stop sending traffic to a backend if it is considered unhealthy. It will start sending traffic back to the server once the probe is healthy again. This ensures that traffic is not being sent to a backend that cannot handle the traffic.

### Scaling

**Design Reference:** Table 4 – [CO4](#_Azure_App_Gateway_1) Table 6 – [PE5](#_Azure_App_Gateway_3)

**Design Decision:** Autoscaling will be enabled for Production workloads.

**Design Justification:** Autoscaling will allow the App Gateway to scale in or out based on application and traffic demands. This allows for cost savings as it will run at lower instance counts when traffic is decreased.It is assumed that any non-production deployment of the App Gateway will not require autoscaling.

### Monitoring

**Design Reference:** Table 5 – [OE1, OE4](#_Azure_App_Gateway_2)

**Design Decision:** NetworkWatcher will be used to enable Network Insights for App Gateway. Capacity should also be monitored for, and alerts set up.

**Design Justification:** Network Insights will be enabled through NetworkWatcher in the same subscription as the App Gateway. This will allow you to capture comprehensive topology and health metrics for network resources, including Application Gateway. This will improve the ability to troubleshoot any issues.

Capacity should be monitored through the metrics portion of the App Gateway deployment. Capacity units represent overall gateway utilization in terms of throughput, compute, and connection count. An alert will be configured if it crosses 75%.

### Logging

**Design Reference:** Microsoft Security Benchmark [LT-4](#_Overview), Table 5 – [OE3](#_Azure_App_Gateway_2)

**Design Decision:** Diagnostic logs will be collected and sent to thecentral log analytics workspace in that region.

**Design Justification:** Diagnostic logs are required to be captured so they can be queried and analysed to assess any performance or health issues.

### Instance Counts

**Design Reference:** Table 6 – [PE2, PE3](#_Azure_App_Gateway_3)

**Design Decision:** A minimum instance count of 2 will be set. The maximum should be defined during application design but is assumed as a default of 10.

**Design Justification:** 2 is recommended as the minimum instance count as this guarantees high availability. A new instance can take 6 to 7 minutes to create, which may not be feasible for Production applications that are required to be always on. The maximum can be set during application design, but a maximum of 10 is assumed as the default. This allows for significant scale-out without overprovisioning and blowing out costs.

### Networking

**Design Reference:** Table 6 – [PE4](#_Azure_App_Gateway_3)

**Design Decision:** A dedicated subnet will be deployed, with a minimum of /26 sizing. The Route Table attached will need an exemption from the standard policy deployment.

**Design Justification:** The standard Route Table policy will not allow the App Gateway to work as intended as it will lead to asymmetric routing. For the V2 deployment, 0.0.0.0/0 sent to a virtual appliance is unsupported.

### Secrets and Credentials

**Design Reference:** Microsoft Security Benchmark [DP-7](#_Overview)

**Design Decision:** If using certificates such as for TLS, it is recommended to store them in a Key Vault.

**Design Justification:** Key Vaults are the most secure native service for storing secrets, credentials and certificates, and are the recommended location for certificates relating to the App Gateway.

### Encryption

**Design Reference:** Microsoft Security Benchmark [DP-3, DP-4](#_Overview)

**Design Decision:** For all applications it is recommended to only use HTTPS and enforce TLS 1.2 for transit.

**Design Justification:** HTTPS and TLS 1.2 are more secure than any earlier form of encrypted traffic, so it is recommended to use these as the default, and modify applications to use these protocols where possible.

# Azure Policies

There are no additional Azure Policies required for this service.

# Configuration Templates

## Primary Production Application Gateway

|  |  |
| --- | --- |
| Configuration Item | Configuration Value |
| **Name** | agw-prd-ause-[appname]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Region** | Australia Southeast |
| **Tier** | WAFV2/StandardV2 |
| **Enable autoscaling** | Yes |
| **Minimum instance count** | 2 |
| **Maximum instance count** | 10 |
| **Availability Zone** | N/A |
| **HTTP2** | Enabled |
| **WAF Policy** | waf-prd-ause-[appname]-01 |
| **Virtual Network** | vnet-prd-ause-[appname]-01 |
| **Subnet** | snet-prd-ause-[appname]-[workload]-01 |
| **Frontend** | Public/Both |
| **Backend Pool** | bep-prd-ause-[appname]-01 |
| **Routing Rule** | rr-prd-ause-https-[appname]-01 |
| **Backend Port** | 443 |
| **Use for app service** | Yes/No |
| **Cookie-based affinity** | Enable/Disable |
| **Connection draining** | Enable/Disable |
| **Request time-out** | 20 (seconds) |
| ***Health Probe Settings*** |  |
| **Name** | hp-prd-ause-[appname]-01 |
| **Protocol** | HTTP/HTTPS |
| **Interval** | 30 |
| **Timeout** | 30 |
| **Unhealthy Threshold** | 3 |
|  |  |

## Secondary DR Application Gateway

|  |  |
| --- | --- |
| Configuration Item | Configuration Value |
| **Name** | agw-dr-auea-[appname]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Region** | Australia East |
| **Tier** | WAFV2/StandardV2 |
| **Enable autoscaling** | Yes |
| **Minimum instance count** | 2 |
| **Maximum instance count** | 10 |
| **Availability Zone** | N/A |
| **HTTP2** | Enabled |
| **WAF Policy** | waf-dr-auea-[appname]-01 |
| **Virtual Network** | vnet-dr-auea-[appname]-01 |
| **Subnet** | snet-dr-auea-[appname]-[workload]-01 |
| **Frontend** | Public/Both |
| **Backend Pool** | bep-dr-auea-[appname]-01 |
| **Routing Rule** | rr-dr-auea-https-[appname]-01 |
| **Backend Port** | 443 |
| **Use for app service** | Yes/No |
| **Cookie-based affinity** | Enable/Disable |
| **Connection draining** | Enable/Disable |
| **Request time-out** | 20 (seconds) |
| ***Health Probe Settings*** |  |
| **Name** | hp-dr-auea-[appname]-01 |
| **Protocol** | HTTP/HTTPS |
| **Interval** | 30 |
| **Timeout** | 30 |
| **Unhealthy Threshold** | 3 |

## Primary Non-Production Application Gateway

|  |  |
| --- | --- |
| Configuration Item | Configuration Value |
| **Name** | agw-[env]-ause-[appname]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Region** | Australia Southeast |
| **Tier** | WAFV2/StandardV2 |
| **Enable autoscaling** | No |
| **Minimum instance count** | 2 |
| **Maximum instance count** | 2 |
| **Availability Zone** | N/A |
| **HTTP2** | Enabled |
| **WAF Policy** | waf-[env]-ause-[appname]-01 |
| **Virtual Network** | vnet-[env]-ause-[appname]-01 |
| **Subnet** | snet-[env]-ause-[appname]-[workload]-01 |
| **Frontend** | Public/Both |
| **Backend Pool** | bep-[env]-ause-[appname]-01 |
| **Routing Rule** | rr-[env]-ause-https-[appname]-01 |
| **Backend Port** | 443 |
| **Use for app service** | Yes/No |
| **Cookie-based affinity** | Enable/Disable |
| **Connection draining** | Enable/Disable |
| **Request time-out** | 20 (seconds) |
| ***Health Probe Settings*** |  |
| **Name** | hp-[env]-ause-[appname]-01 |
| **Protocol** | HTTP/HTTPS |
| **Interval** | 30 |
| **Timeout** | 30 |
| **Unhealthy Threshold** | 3 |

# Acceptance

Signature of this page by appropriately delegated representatives of ​Ambulance Victoria​ signifies acceptance of this design document.

Logicalis will commence build and implementation work once it receives a signed copy of this design document.

Signature of this page by appropriately delegated representatives of Ambulance Victoria signifies acceptance of this design document.

Logicalis will commence build and implementation work once it receives a signed copy of this design document.

|  |  |
| --- | --- |
| Project | Core Services |
| Document Version | 1.0 |

**Signed on behalf of Ambulance Victoria**

|  |  |
| --- | --- |
| Name | Dan Howarth |
| Position |  |
| Signature |  |
| Date signed |  |

**Signed on behalf of Logicalis Australia**

|  |  |
| --- | --- |
| Name | Daniela Nikolic |
| Position | Senior Cloud Engineer |
| Signature |  |
| Date signed |  |

1. https://learn.microsoft.com/en-us/azure/well-architected/ [↑](#footnote-ref-2)
2. https://azure.microsoft.com/en-us/pricing/details/application-gateway/ [↑](#footnote-ref-3)
3. https://learn.microsoft.com/en-us/azure/well-architected/resiliency/overview [↑](#footnote-ref-4)
4. https://learn.microsoft.com/en-us/azure/well-architected/cost/overview [↑](#footnote-ref-5)
5. https://learn.microsoft.com/en-us/azure/well-architected/scalability/overview [↑](#footnote-ref-6)
6. https://learn.microsoft.com/en-us/azure/well-architected/security/security-principles [↑](#footnote-ref-7)
7. https://learn.microsoft.com/en-us/azure/application-gateway/overview [↑](#footnote-ref-8)
8. https://learn.microsoft.com/en-us/azure/application-gateway/features [↑](#footnote-ref-9)
9. https://learn.microsoft.com/en-us/azure/application-gateway/configuration-infrastructure [↑](#footnote-ref-10)