**CORE SERVICE DESIGN:**

**Azure Site Recovery**

atabricks

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

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Azure Site Recovery Core Service Design |
| **File Name** | Ambulance Victoria – Azure Site Recovery Core Service Design v2.0.docx |
| **Version** | 2.0 |
| **Status** | Updated |
| **Release Date** | 21/02/2024 |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 8/02/2024 |
| 2.0 | Updated | Minor feedback | 7, 8, 15, 17, 20, 21 | 21/02/2024 |

Table of Contents

[1. Overview 5](#_Toc159334747)

[1.1 Purpose and Audience 5](#_Toc159334748)

[1.2 Scope and Key Deliverables 5](#_Toc159334749)

[1.3 Glossary and Definitions 6](#_Toc159334750)

[2. Executive Summary 7](#_Toc159334751)

[2.1 Disaster Recovery 8](#_Toc159334752)

[3. Resource Cost 9](#_Toc159334753)

[4. WAF and Security Control Alignment 9](#_Toc159334754)

[4.1 Reliability 10](#_Toc159334755)

[4.1.1 Overview 10](#_Toc159334756)

[4.1.2 Azure Site Recovery Reliability Checklist 10](#_Toc159334757)

[4.2 Cost Optimisation 10](#_Toc159334758)

[4.2.1 Overview 10](#_Toc159334759)

[4.2.2 Azure Site Recovery Cost Optimisation Checklist 10](#_Toc159334760)

[4.3 Operational Excellence 11](#_Toc159334761)

[4.3.1 Overview 11](#_Toc159334762)

[4.3.2 Azure Site Recovery Operational Excellence Checklist 11](#_Toc159334763)

[4.4 Performance Efficiency 11](#_Toc159334764)

[4.4.1 Overview 11](#_Toc159334765)

[4.4.2 Azure Site Recovery Performance Efficiency Checklist 11](#_Toc159334766)

[4.5 Security 12](#_Toc159334767)

[4.5.1 Overview 12](#_Toc159334768)

[4.5.2 Azure Site Recovery Security Checklist 12](#_Toc159334769)

[5. Architecture Summary 14](#_Toc159334770)

[5.1 Resource Overview 14](#_Toc159334771)

[5.2 Solution Diagram 15](#_Toc159334772)

[5.3 RBAC 16](#_Toc159334773)

[5.4 Design Decisions and Justifications 17](#_Toc159334774)

[5.4.1 Azure Site Recovery Regions 17](#_Toc159334775)

[5.4.2 ASR Churn 17](#_Toc159334776)

[5.4.3 Azure Site Recovery Use 17](#_Toc159334777)

[5.4.4 Deploying Azure Site Recovery 18](#_Toc159334778)

[6. Azure Policies 19](#_Toc159334779)

[7. Configuration Templates 20](#_Toc159334780)

[7.1 Azure Policy Settings 20](#_Toc159334781)

[7.2 Platinum Retention Policy Settings 21](#_Toc159334782)

[7.3 Gold/Silver Retention Policy Settings 21](#_Toc159334783)

[8. Acceptance 22](#_Toc159334784)

# Overview

This document covers the baseline design for the Azure Site Recovery 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 Site Recovery 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 Site Recovery.

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 Site Recovery 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 |
| **DR** | Disaster Recovery |
| **DRP** | Disaster Recovery Plan |
| **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 |
| **ASR** | Azure Site Recovery |
| **RTO** | Recovery Time Objective |
| **RPO** | Recovery Point Objective |

Table 1: Glossary and definitions

# Executive Summary

This design covers the baseline standards for the Azure Site Recovery 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 Security was relevant. Azure Site Recovery is not something that is deployed and configured itself, but rather configured as a part of another deployment (Virtual Machines as an example). As such the following recommendations have been put forward:

* ASR will be used for Production workloads.
* Recovery for other services, even Platinum services, can also be done with Azure Backup
* Assess per workload if ASR is required to be configured
* Test ASR against pre-defined RTO and RPO targets
* Do not configure ASR for Non-Production or Bronze workloads

This service is configured the same regardless of the service catalog tier of the workload being protected so there is no difference in configuration.

Note that one **major deviation** from other services is that ASR cannot be deployed through Bicep. It must be configured manually through the portal, through PowerShell, or an Azure Policy can be implemented, though it is not recommended to force all new Virtual Machines to use this policy and should be done knowing that there is a specific requirement that ASR can meet.

## Disaster Recovery

Note that ASR on its own does **NOT** meet Disaster Recovery requirements, only the infrastructure failover for Virtual Machines. An overall Disaster Recovery and Business Continuity agenda needs to be created considering not only how to recover each application, but also the order in which applications need to be brought back ordered by priority.

Each application should have its own individual runbook as well as regular failover testing to ensure that it can be recovered in case of component failover, as well as in the case of a full regional outage.

Some components to be considered for an overall Disaster Recovery runbook and planning are:

* ASR and backup enablement of infrastructure
* Application layer requirements and sequencing
* RTO and RPO definitions
* Failover test planning
* Communications plans
* Application recovery prioritisation
* Updated DRP for each application landing zone design
* Recovery type for each application: active-active, active-passive etc.
* Whether the application needs recovery or if it has innate availability

**Additional References:**

* [Pages - Guides, Tools and Templates (ambulance.vic.gov.au)](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fintranet.ambulance.vic.gov.au%2Fsites%2FTeams%2Fem%2Fbr%2FPages%2FGuides--Tools.aspx&data=05%7C02%7Cven1tddn%40AMBULANCE.VIC.GOV.AU%7Cfa4918b51b6548d5c80208dc31a8c37e%7C86b0e251f8cb4d7aabd236a8896457e7%7C0%7C0%7C638439848107345699%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=AJUAGRqZA%2Br0p%2FSarndK88dtAxWbl747s26IYMt3Oyw%3D&reserved=0)
* [https://intranet.ambulance.vic.gov.au/procedures/Procedures/PRO%20TAS%20004%20Data%20Backup.pdf](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fintranet.ambulance.vic.gov.au%2Fprocedures%2FProcedures%2FPRO%2520TAS%2520004%2520Data%2520Backup.pdf%23search%3Drecovery&data=05%7C02%7Cven1tddn%40AMBULANCE.VIC.GOV.AU%7Cfa4918b51b6548d5c80208dc31a8c37e%7C86b0e251f8cb4d7aabd236a8896457e7%7C0%7C0%7C638439848107360478%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=iZKnqBfZ1wXJyBkd8Gi%2BysaNCmyiBK6JPm%2BpdfgvWrM%3D&reserved=0)
* [https://intranet.ambulance.vic.gov.au/procedures/Procedures/FRA%20DTS%20001%20DTS%20Business%20Service%20Catalogue.pdf](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fintranet.ambulance.vic.gov.au%2Fprocedures%2FProcedures%2FFRA%2520DTS%2520001%2520DTS%2520Business%2520Service%2520Catalogue.pdf%23search%3Drecovery&data=05%7C02%7Cven1tddn%40AMBULANCE.VIC.GOV.AU%7Cfa4918b51b6548d5c80208dc31a8c37e%7C86b0e251f8cb4d7aabd236a8896457e7%7C0%7C0%7C638439848107371428%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=GbKUL0hLiCRNiYQOamwgAT9umCJGNYL2q%2BxWxYT4eRk%3D&reserved=0)
* [https://intranet.ambulance.vic.gov.au/procedures/Procedures/POL%20FCS%20079%20Business%20Resilience%20Policy.pdf](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fintranet.ambulance.vic.gov.au%2Fprocedures%2FProcedures%2FPOL%2520FCS%2520079%2520Business%2520Resilience%2520Policy.pdf%23search%3Drecovery&data=05%7C02%7Cven1tddn%40AMBULANCE.VIC.GOV.AU%7Cfa4918b51b6548d5c80208dc31a8c37e%7C86b0e251f8cb4d7aabd236a8896457e7%7C0%7C0%7C638439848107382868%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=Wc%2ByO8ZzDf06msbHs6j3Jejc5pAkcp8ENvLyCUsAGQA%3D&reserved=0)
* [https://intranet.ambulance.vic.gov.au/sites/Teams/IT/ICT%20Documentation/Cybersecurity%20Policies%20and%20Standards%20Implementation/POL%20DTS%20001%20Backup%20and%20Recovery%20Policy.pdf](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fintranet.ambulance.vic.gov.au%2Fsites%2FTeams%2FIT%2FICT%2520Documentation%2FCybersecurity%2520Policies%2520and%2520Standards%2520Implementation%2FPOL%2520DTS%2520001%2520Backup%2520and%2520Recovery%2520Policy.pdf%23search%3DPOL%252FDTS&data=05%7C02%7Cven1tddn%40AMBULANCE.VIC.GOV.AU%7Cfa4918b51b6548d5c80208dc31a8c37e%7C86b0e251f8cb4d7aabd236a8896457e7%7C0%7C0%7C638439848107393493%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=Cudk%2BX6Fak%2BxNyvhKD6P2Z7imEafzNgTNAY7%2BdK8ldU%3D&reserved=0)

# Resource Cost

The following table shows the pricing construct for Azure Site Recovery[[2]](#footnote-3):

|  |  |  |
| --- | --- | --- |
|  | Price For First 31 days | Price After 31 Days |
| Azure Site Recovery to customer owned sites | Free | **$23.360**/month per instance protected |
| Azure Site Recovery to Azure | Free | **$36.500**/month per instance protected |

Table : 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 Site Recovery Reliability Checklist

There is no specific Reliability guidance for Azure Site Recovery as this service inherently supports other services and applications achieve their reliability targets and manages potential failure.

## 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 Site Recovery Cost Optimisation Checklist

There is no specific guidance for Azure Site Recovery with respect to Cost Optimisation as there are no options to reduce the cost of the service. The only commentary is to ensure that the applications and workloads that leverage Azure Site Recovery do require it as the cost is per protected instance. This example is for Virtual Machines, replace for the relevant resource:

## 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 Site Recovery Operational Excellence Checklist

There is no specific Operational Excellence guidance for Azure Site Recovery as this service inherently supports other services and applications achieve their Operational Excellence targets and manages potential failure.

## 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 Site Recovery Performance Efficiency Checklist

There is no specific Performance Efficiency guidance for Azure Site Recovery as this service inherently supports other services and applications achieve their Performance Efficiency targets and manages potential failure.

## 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.

### Azure Site Recovery Security Checklist

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | DH Ref. | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **S1** | 19.1.1 | Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | Yes | No | Governance | Operational - annually |
| **S2** | 19.2.2 | Maintain a physically separate recovery site that enables ready restoration of key systems in the event that their availability is lost. | Yes | Yes | IaC | At deployment |
| **S3** | 5.1.2 | Restoration of important data, software and configuration settings from backups to a common point of time is tested as part of disaster recovery exercises. | Yes | No | Governance | Operational – quarterly |
| **S4** | 19.1.3 | Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets. | Yes | No | Governance | Operational - quarterly |

Table 7: Security checklist summary

# Architecture Summary

## Resource Overview

Azure Site Recovery is an Azure native service that supports a BCDR (Business Continuity and Disaster Recovery) strategy for planned and unplanned outages[[7]](#footnote-8). It allows you to manage replication, failover, and failback for services that have this enabled. It can be used for Azure VMs as well as On-Premises replication. It also enables you to test Disaster Recovery and run drills without impacting the live replication of machines.

Failovers can also be customised to ensure that the sequence of multi-tiered applications is failed over correctly.

## Solution Diagram

Figure : ASR from Primary Region to Secondary Region

## RBAC

For Azure Site Recovery the following roles are applicable[[8]](#footnote-9):

|  |  |
| --- | --- |
| Role Name | Description |
| Site Recovery Contributor | Lets you manage Site Recovery service except vault creation and role assignment. |
| Site Recovery Operator | Lets you failover and failback but not perform other Site Recovery management operations. |
| Site Recovery Reader | Lets you view Site Recovery status but not perform other management operations. |

Table : 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 Site Recovery 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.

### Azure Site Recovery Regions

**Design Reference:** Table 7 – [S2](#_Azure_Site_Recovery)

**Design Decision:** Australia East is the Disaster Recovery region.

**Design Justification:** Australia Southeast is architecturally the Primary Region for Ambulance Victoria. ASR should be configured to failover to the Disaster Recovery region in Australia East, unless otherwise approved and required for a specific application deployment. This also meets the security control of having two physically separate regions for recovery.

### ASR Churn

**Design Reference:** N/A

**Design Decision:** Churn support will not be enabled by default, and only enabled for workloads that require it.

**Design Justification:** Churn is the data change rate, and the default supported by ASR is 54 MB/s per VM[[9]](#footnote-10). The High churn option can be enabled manually in the portal if the workload to be replicated has a High Churn requirement. High Churn supports workloads up to 100MB/s.

### Azure Site Recovery Use

**Design Reference:** Table 7 - [S1, S3](#_Azure_Site_Recovery)

**Design Decision**: Azure Site Recovery should be used for applications that have specific RTO and RPO requirements. It should be applied to Production workloads.

**Design Justification**: It is not recommended to have ASR configured for every workload as a default. Even for Platinum workloads it should be assessed and tested against RTO and RPO. It is recommended to enable for Platinum workloads. For Gold and Silver workloads it should be considered a case-by-case enablement. It is not recommended for Non-Production workloads.

### Deploying Azure Site Recovery

**Design Reference:** N/A

**Design Decision:** Azure Site Recovery should be used for applications that have specific RTO and RPO requirements. It is assumed that this will most likely be Platinum workloads.

**Design Justification:** The capability to deploy the service directly with Bicep does not exist, so it must be done through another form of scripting such as PowerShell, or through Azure Policy. Azure Policy is the recommended method as there is already a built-in Policy, as defined in Section 6. If Azure Policy is to be used it can be applied at the root management group, and the settings should specify that only machines with a specific tag have this capability enabled.

# Azure Policies

The following built-in Azure Policy may be used if it is preferable to using PowerShell during deployments:

|  |  |
| --- | --- |
| Policy Name | Description |
| Configure disaster recovery on virtual machines by enabling replication via Azure Site Recovery | Virtual machines without disaster recovery configurations are vulnerable to outages and other disruptions. If the virtual machine does not already have disaster recovery configured, this would initiate the same by enabling replication using preset configurations to facilitate business continuity. You can optionally include/exclude virtual machines containing a specified tag to control the scope of assignment. |

For this Policy it is recommended to apply to Production Virtual Machines. The settings within this policy can be configured so that only machines with a specific tag will have this enabled. As discussed in this document, ASR is not recommended to be the default enablement across all servers, only specific servers that have this as a requirement.

# Configuration Templates

The following configuration template varies slightly from other documents. The below shows how to configure the Azure Policy recommended to enable ASR on Virtual Machines.

## Azure Policy Settings

|  |  |
| --- | --- |
| Policy Parameter | Setting |
| **Scope** | The Management Group, Subscription, or Resource Group that the Policy is assigned to. |
| **Exclusions** | Any Management Group, Subscription, or Resource Group required to be exempted from the policy |
| **Source Region** | Australia Southeast |
| **Target Region** | Australia East |
| **Target Resource Group** | The resource group that will host the Virtual Machine that will be created in the Disaster Recovery region |
| **Vault Resource Group** | The resource group that hosts the Recovery Services vault to be used for a given deployment |
| **Recovery Service Vault** | The name of the Recovery Services Vault supporting ASR for a given deployment |
| **Remediation** | Check the box for Create a remediation task |
| **Managed Identity** | Check the box to create a Managed Identity |
| **Type of Managed Identity** | System Assigned |
| **Managed Identity Location** | Australia Southeast |
| **Tag Type** | Inclusion |
| **Tag Name** | ASR\_Enabled\_Platinum  or  ASR\_Enabled\_GoldSilver |
| **Tag Value** | Yes |

## Platinum Retention Policy Settings

|  |  |
| --- | --- |
| Configuration Item | Configuration Setting |
| **Name** | Platinum\_ASR\_RetentionPolicy |
| **Retention Period (in days)** | 15 |
| **App Consistent Snapshots (hours)** | 4 |
| **Automation Account** | aa-prd-auea-[appname]-asr-01 |

## Gold/Silver Retention Policy Settings

|  |  |
| --- | --- |
| Configuration Item | Configuration Setting |
| **Name** | GoldSIlver\_ASR\_RetentionPolicy |
| **Retention Period (in days)** | 7 |
| **App Consistent Snapshots (hours)** | 8 |
| **Automation Account** | aa-prd-auea-[appname]-asr-01 |

# 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-gb/pricing/details/site-recovery/ [↑](#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/site-recovery/site-recovery-overview [↑](#footnote-ref-8)
8. https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles [↑](#footnote-ref-9)
9. https://learn.microsoft.com/en-us/azure/site-recovery/concepts-azure-to-azure-high-churn-support [↑](#footnote-ref-10)