Version 0.1

Prepared by

Principal Consultant

someone@microsoft.com

Contributors

Sam Boulad, Matt Wiscombe

Revision and Signoff Sheet

Change Record

Date	Author	Version	Change Reference
6/6/2025		0.1	Initial draft for review/discussion

Reviewers

Date	Name	Version Approved	Position
		0.1	Digital Architect

Table of Contents

1 Introduction

The Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) has a commitment to deliver technology and innovation that enables operations and capability for the Australian Government. As part of this commitment, the Chief Information Officer Group (CIOG) is establishing the ability to consume enterprise-ready cloud services via standardised and patterned means.

DITRDCA has engaged Microsoft to assist CIOG's Cloud Center of Excellence (CCoE) group to design and deploy a robust cloud foundation using Microsoft Azure, to support current and future cloud workloads. This program of work is referred to as Azure Cloud Foundations (ACF).

This engagement encompasses the modernization of existing DMZ infrastructure, integration of on-premises Microsoft Active Directory, migration of web and application servers, and the implementation of Microsoft Defender for Cloud Apps as part of a comprehensive security posture aligned with Australian Government ISM PROTECTED controls and Essential Eight strategies.

- The foundation is built upon Microsoft's Cloud Adoption Framework (CAF) Landing Zone Design Areas, ensuring a structured, secure, and compliant approach to cloud adoption that meets the stringent requirements of Australian Federal Government operations Governance, policy and compliance;
- Account and subscription hierarchy; and
- Foundational cloud services, including Azure Compute, Storage, Networking, Identity and Security

The intent of this Design and Plan document is to align with Microsoft’s Virtual Data Center (VDC) concept. VDC leverages a ‘hub and spoke’ deployment model to maximise flexibility and scalability while supporting enhanced security, governance and compliance in an organisation’s cloud environment

The outcomes for DITRDCA will be the implementation of a hybrid cloud deployment which will deliver capability to establish a secure boundary around any systems and applications deployed into Azure in the future. The 'hub' provides the consistent security, connectivity and policy enforcement required for the DITRDCA environment and will enable confident execution of development, test and ultimately production activities in the associated 'spokes'.

> Note:
>
> Further information on the CAF

1.1 Project Overview

DITRDCA has engaged Microsoft Services to provide a comprehensive design document that can be used for both Azure Cloud Foundations deployment and Microsoft Defender for Cloud Apps (Platform) deployment. This document details the design and plan for the following components of the project:

Core Infrastructure Components

- Azure Landing Zones: CAF-aligned landing zones for production and non-production workloads
- DMZ Modernization: Uplift of existing perimeter security architecture
- Hybrid Identity: Integration of on-premises Active Directory with Azure AD
- Network Architecture: Hub-and-spoke topology with secure connectivity

Security Platform Components

- Microsoft Defender for Cloud Apps: Cloud access security broker (CASB) implementation
- Microsoft Defender for Endpoint: Endpoint detection and response integration
- Microsoft Entra ID: Identity and access management integration
- Microsoft XDR: Extended detection and response integration

Migration Components

- Web Server Migration: Modernization of existing web applications
- Application Server Migration: Migration of business applications with hybrid connectivity
- Database Migration: Secure migration of data assets to Azure SQL services

- Legacy Integration: Secure connectivity for applications requiring on-premises access

1.2 Intended Audience

The Design and Plan has been prepared for a technical audience, specifically:

Primary Audience

- Chief Information Officer Group (CIOG) Architect Team: Strategic architecture guidance and decision-making
- CIOG Security Team: Security architecture, controls implementation, and compliance validation
- Cloud Center of Excellence (CCoE): Cloud adoption strategy and operational excellence

Secondary Audience

- Technical Architecture Teams: Infrastructure design and implementation guidance
- Security Operations Teams: Security monitoring, incident response, and threat management
- Network Operations Teams: Network architecture, connectivity, and performance management
- Database Administration Teams: Data migration, security, and operational procedures
- Application Development Teams: Application modernization and cloud-native development practices

Stakeholder Groups

- Compliance and Risk Teams: Regulatory compliance and risk management oversight
- Project Management Office: Project delivery coordination and governance
- Vendor Management Teams: Third-party integration and service management

> **Note**
>
> Please refer to the DMZ document high-level overview of the VDC concept and how that will support and integrate with DITRDCA broader environment.

1.3 Purpose of the document

This document serves as the comprehensive design and implementation guide for DITRDCA's Azure Cloud Foundations initiative. The primary purposes include:

Strategic Guidance

- Provide architectural blueprints aligned with Microsoft Cloud Adoption Framework
- Establish governance framework for ongoing cloud adoption
- Define security posture requirements for ISM PROTECTED workloads

Technical Documentation

- Detail specific Azure service configurations and integrations
- Document network architecture and security control implementations
- Provide step-by-step implementation procedures and best practices

Compliance Framework

- Map ISM PROTECTED controls to Azure native security services
- Demonstrate Essential Eight strategy implementation in cloud environment
- Establish continuous compliance monitoring and reporting mechanisms

Knowledge Transfer

- Enable DITRDCA teams to self-manage and extend the cloud foundation
- Provide operational runbooks and troubleshooting procedures
- Establish training framework for ongoing capability development

The Design and Plan identifies, where applicable, any additional infrastructure requirements and implications for connectivity, authentication and management to enable creation of new production workloads in Azure (or any future migration of existing on-premises workloads into Azure).

1.4 Scope of the Design and Plan document

The Design and Plan is focused on foundational aspects of DITRDCA Azure implementation and describes technical design details and the high-level implementation plan. The Design and Plan

describes the Azure IaaS and PaaS services in scope and the integration capabilities each offers at a high-level, however, not every service and capability within Azure will be covered. DITRDCA may look at additional or new features in Azure, as and when required.

The services in Azure that are in scope of cloud foundations are included in this document and will be sufficient to provide the reader with a basic understanding of the service(s) and their implementation, however, detailed technical deployment, or DITRDCA specific settings for these services will be scoped in appending documentation, or addressed in future engagements (as applicable to the scope of this engagement).

1.4.1 In Scope

The following are in scope for the Design and Plan:

- A DITRDCA Azure hybrid cloud design based on Virtual Data Center (VDC) pattern to provide a foundational Azure platform that is to be accredited to PROTECTED
- Detail of Azure based services for Cloud Foundations;
- Provision of a list of details and recommendations for each of the concepts and Azure services where applicable; and
- Documentation of DITRDCA design decisions from the 'Insights and Design' workshops conducted as part of the ACF engagement.
- Assist in uplifting DMZ and perimeter security posture to meet current and future cloud security requirements.

  - Support the design and implementation of Azure Landing Zones aligned to Microsoft's Cloud Adoption Framework.

- Assist with the deployment and configuration of laaS environments, if deemed necessary for transitional or long-term workload hosting.

- Provide ad hoc technical and architectural support as directed by the

1.4.2 Out of Scope

The following is out of scope for this document:

- Re-design of the delivered via the oobe Perimeta solution (Note: this is a VDC based design);

- Design or/ re-design of DITRDCA operational processes;
- Design or/ re-design of DITRDCA DevOps practices and tooling;
- Design or/ re-design of existing Azure Resource Manager (ARM) templates;
- Design and/or deployment of Privileged Access Workstations (PAWs);
- Design or/ re-design of pre-requisites and supporting technologies, services and platforms including:
    - Network and/or internet connectivity
    - Hardware (for example, servers, storage and networking and security equipment)
    - Existing on-premises or 3rd party identity systems
- Detailed-level documentation of VDC security controls for DITRDCA certification/accreditation processes (as this is addressed by oobe Perimeta);
- Development/review of existing code; and
- Anything not mentioned 'in scope'

Technical Exclusions

- Development or review of existing application code
- Detailed security control documentation for certification processes (leverages existing Azure compliance frameworks)
- Integration with non-Microsoft security tools and platforms
- Custom application development or modification services

1.5 References

The following are documents which are related to this document and may be referred to:

Document	Description
Information Security Manual (ISM)	Australian Signals Directorate - Information security manual (ISM)
Essential Eight Maturity Model	Australian Signals Directorate - Essential Eight maturity model
PSPF	Protective Security Policy Framework

Document	Description
Standards	
Cloud Adoption Framework – Landing Zone Design Areas	
Cloud Adoption Framework - Landing Zone Design Areas	
Azure Security Benchmark	Microsoft's security baseline recommendations for Azure services

Table 1: References

> Note:
>
> The

1.6 Requirements TBC

Requirement ID	Category	Requirement Description	Justification/Rationale	Dependencies/Prerequisites	Related Design Decision(s)
REQ-NET-001	Networking	Define and implement secure network	Ensures isolation, limits lateral movement, and	Azure Virtual Network, NSGs, Azure Firewall	DD-NET-001

		segmentation for DMZ workloads in Azure.	supports ISM/Essential 8 requirements.		
REQ-IDM-001	Identity	Integrate Azure AD with on-premises AD (hybrid identity) and enforce MFA.	Centralizes identity, supports SSO, and meets Essential 8/ISM identity controls.	Azure AD Connect, Conditional Access	DD-IDM-001
REQ-SEC-001	Security	Implement end-to-end encryption for data at rest and in transit.	Protects sensitive data, aligns with ISM/Essential 8 encryption mandates.	Azure Key Vault, TLS, Storage encryption	DD-SEC-001
REQ-COM-001	Compliance	Map ISM and Essential 8 controls to Azure policies and enforce via Azure Policy.	Ensures regulatory compliance and continuous control enforcement.	Azure Policy, Regulatory Compliance Blueprints	DD-COM-001
REQ-MON-001	Monitoring	Deploy centralized logging, monitoring, and alerting for migrated workloads.	Enables visibility, rapid incident response, and ongoing compliance monitoring.	Azure Monitor, Log Analytics, Sentinel	DD-MON-001
REQ-APP-001	Application	Harden migrated applications and apply just-in-time access controls.	Reduces attack surface, supports application hardening (Essential 8), and limits privileged access.	Azure Security Center, JIT VM access	DD-APP-001
REQ-INT-001	Integration	Ensure secure connectivity for applications requiring on-premises access.	Maintains business continuity and secure hybrid operations.	VPN Gateway, ExpressRoute, Private Link	DD-INT-001
REQ-BKP-001	Backup/Recovery	Implement automated, immutable backups and test restore procedures.	Supports Essential 8 backup controls and disaster recovery readiness.	Azure Backup, Recovery Services Vault	DD-BKP-001

REQ-OPS-001	Operations	Define operational processes for patching, vulnerability management, and change control.	Supports Essential 8 patching, reduces vulnerabilities, and ensures operational maturity.	Azure Update Management, Change Tracking	DD-OPS-001

The deployment of Microsoft Defender for Cloud Apps is driven by specific organisational security and operational requirements. These requirements ensure that the solution is configured to address identified risks and align with the overall security strategy.

The following table summarizes the key security, and compliance requirements that guided the design detailed in this report. Each requirement references the specific section(s) where it is addressed.

2 Objectives, Constraints and Assumptions

2.1 Design Objectives

The following objectives are applicable for this design:

Number	Objective

2.2 Design Constraints

The following constraints are applicable and therefore influence this design:

Table 2: Design Constraints

2.3 Design Assumptions

The following design assumptions were made in the ACF workshops and influence this design:

Number	Objective

Table 3: Design Assumptions

1.

3 DITRDCA – Current Environment(s)

Put pic

Figure 1: DITRDCA Current Azure Hub and Spoke environment

4 Design Decisions

During the 'Insights and Discovery' workshops, which were conducted as part of ACF, the design decisions and recommendations were documented.

The design decisions are provided in the table below, referencing the following legend;

- **Microsoft recommends:** Provided for discussion points where DITRDCA did not necessarily have a formal stance due to either: a lack of knowledge of a subject area or no relevant representatives being present.
- **DITRDCA agreed:** Provided for discussion points where DITRDCA agreed with the content presented by Microsoft during the workshop.
- **DITRDCA decided:** Provided for discussion points where DITRDCA already had a formal stance on the subject area including overriding enterprise wide policy or directions outside of the Azure Cloud Foundation project.

Number	Category	Design Decisions/Recommendations
DD-00	Account, Dept, Subscription model	Microsoft recommends maintaining the current structure (based on current approach/process) with expansion out for other groups and services
DD-00	Azure Regions	DITRDCA agreed to deploy ACF in AUCentral regions and AUEast region.
DD-00	Resource Groups	Microsoft recommends DITRDCA use a common pattern or structure for resource groups
DD-00	Cost Management	Microsoft recommends using Azure Cost management as the strategy and solution
DD-00	Identity and Access Management	
DD-0	Identity and Access Management	Microsoft recommends using Azure MFA. DITRDCA agreed Azure MFA should be used in the interim noting phone access restrictions. (Interim decision).

Number	Category	Design Decisions/Recommendations
DD-	Network	Microsoft recommends the hybrid model approach. Microsoft recommends aligning with the VDC concept using hub and spoke in the interim.
DD-0	DevOps	Microsoft recommends embedding security checks as part of DevSecOps to expand on the DevOps methodology for CI/CD pipelines. DITRDCA agreed to keep using the existing process where security controls/validations requirements are defined at the org level and dev teams decide how to perform validation.
DD-0	SIEM	Microsoft recommends using cloud-native tools/solution such as Azure Security Center and Azure Log Analytics workspaces to store events and logs to feed to Azure Sentinel SIEM or on-prem SIEM.
DD-0	Patch Management	Microsoft recommends a ring topology for patch deployment however need more information on existing environment.
DD-0	Encryption	Microsoft recommends encryption be employed both at rest and in-transit required as per ISM controls. Microsoft recommends leveraging Azure Security Center to receive alerts around encryption. DITRDCA agreed it wants crypto at rest and in transit . DITRDCA agreed it wants alerts around encryption. DITRDCA agreed that encryption is enabled for Perimeta resources (IPsec VPN ExpressRoute is the current state). DITRDCA agreed to use Security Center to monitor for bit locker disk encryption.
DD-0	*Key Management*	Microsoft recommends leveraging Azure Key Vault for secret and key management. Microsoft recommends defining a key and secrets management process.

Number	Category	Design Decisions/Recommendations
DD-0	Backup	Microsoft recommends establishing a Cloud backup strategy to suit the different options and requirements to protect IaaS and PaaS. Microsoft recommends using cloud native tools to protect IaaS and PaaS. on-premises into consideration.
DD-0	Monitoring and Alerting	Microsoft recommends leveraging native cloud toolsets (i.e. Azure Monitor with Azure Log Analytics workspaces and Network Watcher). DITRDCA agreed to leverage cloud native tools as part of Perimeta for the ACF interim state. DITRDCA agreed there are multiple teams and tools that integrate with ServiceDesk, email, webpages to alert and notify DPS and Service Management teams.
DD-0	Monitoring and Alerting	Microsoft recommends leveraging native cloud toolsets (i.e. Azure Monitor with Azure Log Analytics workspaces and Network Watcher). DITRDCA agreed to leverage cloud native tools as part of Perimeta for the ACF interim state. DITRDCA agreed there are multiple teams and tools that integrate with ServiceDesk, email, webpages to alert and notify DPS and Service Management teams.
DD-0	Monitoring and Alerting	DITRDCA agreed to leverage native cloud toolsets (i.e. Azure Log Analytics workspaces).
DD-0	Monitoring and Alerting	DITRDCA agreed to leverage native cloud toolsets (i.e. Azure Monitor and Azure Log Analytics workspaces). DITRDCA agreed to leverage specific Azure Monitor solution sets for additional insights (i.e. AD, SQL etc). DITRDCA agreed to use the initial Perimeta and ACF monitoring as a minimum and will build out as applicable.

Number	Category	Design Decisions/Recommendations
DD-0	Monitoring and Alerting	DITRDCA agreed to leverage native cloud toolsets (i.e. Azure Service Maps) with Log Analytics to assist with creating Application Services Maps. DITRDCA will turn on features when needed such as Application Service Maps, depending on cost and who needs them.
DD-0	Backup Strategy	agreed to leverage native cloud toolsets (i.e. Azure Backup) for IaaS workloads. agreed to leverage backup capabilities per Azure PaaS service.
DD-0	Data Retention	agreed to leverage native cloud toolsets (i.e. Azure Backup) for IaaS workloads. agreed to leverage backup capabilities per Azure PaaS service.
DD-0	Backup Service	agreed that Azure Backup will be provided as standard for all 'spokes'.
DD-0	Backup Requirements	Microsoft recommends that AUCentral and AUCentral2 be used by workloads that have a HA/Active-Active requirement. This should be implemented on a workload-by-workload basis. review
DD-	Cost Management Tagging	tags should enable Directorate/Project Owner/Executive get visibility of cost data and should support delegation.
DD-0	Cost Optimisation	agreed that the responsibility for optimisations will come with maturity. It will start as decentralised and then move towards come centralised control.

Table 4: Design Decisions

> **Note:**
>
> The complete list of design decisions including additional details regarding the workshop and questions asked is available in the *DITRDCA CIOG – ACF Design Decisions.xlsx* document.

5 Solution Overview

5.1 Overview

This section provides an overview of the DITRDCA Azure Cloud Foundation platform as part of its hybrid cloud capability. This platform is expected to be formally and centrally approved and managed by DITRDCA to ensure that appropriate governance and security guard rails and controls are built into the environment from the beginning.

The platform is based on a VDC design to enable the environment to be managed via Infrastructure-as-Code (IaC) for simple and repeatable scaling scenarios. For example; additional Azure regions can be provisioned via hub constructs and on-demand workloads hosting via spoke constructs.

6 . Core Framework & Landing Zone Structure

- CAF-Aligned Hub-and-Spoke Topology
- Hub VNet: Centralized shared services (Azure Firewall Premium, DNS forwarders, Bastion Host, DDoS Protection Standard, Log Analytics workspace, Azure Key Vault).
- Spoke VNets: Segregated by workload/application (e.g., AD DMZ, application tiers, management, migration).
- ExpressRoute: Dedicated, private, high-speed connectivity between on-premises and Azure, with IPsec/MACsec encryption as required.
- User Defined Routes (UDRs): All internet-bound traffic is routed through on-premises Secure Internet Gateway (SIG).

Departmental Input Required:

- What is the specific list of server workloads, their functions, criticality, and dependencies that need to be migrated or integrated?
- What are the specific workloads and their migration priorities?
- What are the required downtime windows and migration schedules for specific applications?

7 Management & Governance

- Management Groups: Hierarchical structure reflecting department org units, supporting policy inheritance and centralized governance.
- Azure Policy:
- Enforce ISM and Essential Eight controls.
- Restrict allowed regions and SKUs.
- Require resource tagging for chargeback/showback.
- Role-Based Access Control (RBAC):
- Granular access using built-in roles.
- Privileged Identity Management (PIM) for JIT access.
- Regular Access Reviews for privileged roles.
- Change Management:
- Integrated with existing ITIL/government processes.
- Automated via Azure DevOps pipelines and Infrastructure-as-Code (ARM/Bicep).

Departmental Input Required:

- What is the specific Management Group hierarchy structure that aligns with the department's organizational structure and desired policy/governance boundaries?
- What is the exact list of allowed Azure regions that resources can be deployed into?
- What is the exact list of allowed SKUs (e.g., VM sizes, database tiers) for various resource types?
- What is the required Information Security Manual (ISM) level and Essential Eight maturity level that the environment must adhere to?
- What are the specific compliance requirements, policies, and audit requirements beyond the standard ISM/Essential Eight frameworks?
- What are the department's specific governance policies and escalation paths for non-compliance or incidents?
- What are the department's specific change management processes that must be integrated into the cloud operations?

- What are the specific cost management requirements, including chargeback/showback models?
- What are the tagging standards that must be enforced for resource groups and resources?
- What is the policy definition ID for the official ISM/Essential Eight policy set to be assigned?

8

9 Identity & Access

- Identity Modernisation:
- Microsoft Entra ID (Azure AD) as primary identity provider.
- Federated authentication via ADFS; MFA enforced with smart cards/hard tokens.
- Azure AD Connect for hybrid sync (excluding privileged accounts).
- Conditional Access:
- Risk-based policies for all users.
- Device compliance integration with Microsoft Intune.
- RBAC Expansion:
- Existing ARM RBAC model extended to new workloads and landing zones.

Departmental Input Required:

- What are the specific user roles and group memberships that need to be configured in Azure AD and synchronized from on-premises?
- What are the detailed requirements for privileged access needs and their corresponding PIM configurations?
- How should Azure AD Conditional Access policies be specifically configured for government-grade authentication, including PIV card integration requirements?

4. Networking & Security

- Network Segmentation:
- NSGs and ASGs for subnet/VM-level micro-segmentation.
- Dedicated subnets for DMZ replacement, application, management, and migration.
- Firewall & Load Balancing:
- Azure Firewall Premium in hub for central policy enforcement.
- Azure Application Gateway with WAF for web-facing workloads.
- Azure Load Balancer for internal and external load balancing as needed.
- DDoS Protection Standard:
- Enabled on all public endpoints and critical VNets.

- Private Endpoints:
- Used for all PaaS services (Key Vault, SQL, Storage) to restrict public access.
- ExpressRoute Encryption:
- IPsec tunnels or MACsec for sensitive traffic.
- F5 Functionality:
- Replaced by Azure Application Gateway and Azure Firewall, with custom rules for legacy app support if needed.

Departmental Input Required:

- What is the department's complete and detailed IP addressing scheme to be used in Azure (VNet ranges, subnet ranges)?
- What is the required number and purpose of subnets within the VNets (e.g., DMZ replacement, application tiers, management, migration)?
- What are the detailed network requirements for the servers/workloads to be migrated (e.g., specific ports, protocols, dependencies)?
- Which public endpoints need DDoS Protection Standard enabled?
- How will the existing firewall and F5 load balancer functionality be replicated or replaced in Azure?

10 Workload Landing Zones

- Active Directory DMZ:
- Domain controllers in a dedicated spoke, with NSGs restricting access.
- Replication traffic filtered and monitored.
- Web Application Zone:
- Azure App Service (PaaS) integrated with VNet.
- Application Gateway with WAF for inbound HTTPS.
- Key Vault for certificate management.
- Database Zone:
- Azure SQL Managed Instance or SQL VM with TDE, Always Encrypted, TLS 1.3.
- Key Vault with HSM for key management.
- Hybrid Integration Zone:
- Azure Arc for on-premises server management.
- ExpressRoute/S2S VPN for hybrid connectivity.

Departmental Input Required:

- What are the detailed data classification requirements for the data that will reside in Azure?
- What are the department's specific business continuity and disaster recovery needs and requirements (RTO/RPO)?
- What are the specific backup and retention policies for different types of data and workloads?
- What are the backup frequency requirements and the list of critical workloads requiring specific backup/DR configurations?

6. Security Architecture

- Zero Trust Model:
- Conditional Access, Defender for Identity, Intune device compliance.
- Data Protection:

- Microsoft Purview and Azure Information Protection for data classification and labeling.
- Encryption at rest and in transit for all workloads.
- SOC Integration:
- Microsoft Sentinel SIEM for centralized log collection, analytics, and SOAR playbooks.
- Integration with government incident response workflows.
- Key Management:
- Azure Key Vault (with HSM as required) in each hub/spoke.
- Service endpoints for secure access.

Departmental Input Required:

- What are the specific security operations contacts and their roles in monitoring and incident response?
- What are the specific details required for SIEM integration, including the SIEM endpoint details if it's not Azure Sentinel, and log access policies?
- What are the specific list of secrets, keys, and certificates that need to be secured in Azure Key Vault for workloads?
- What are the specific requirements for Azure Key Vault HSM integration for FIPS 140-2 Level 3 compliance?
- What are the specific requirements for Automated Response and Remediation playbooks and their integration with existing government service management systems?

11

12 Operations & Monitoring

- Monitoring & Observability:
- Azure Monitor, Log Analytics, and Application Insights for performance, health, and security.
- Network Performance Monitor in a separate workspace.
- Automation:
- Azure Automation, DSC, Logic Apps, and Functions for operational tasks and event-driven workflows.
- Backup & DR:
- Azure Backup and Recovery Services Vaults in each region.
- Azure Site Recovery for cross-region DR.
- Immutable backup storage for ransomware resilience.

Departmental Input Required:

- What is the required retention period for logs in Log Analytics?
- What are the department's SLA expectations for different workloads and services?
- What are the required maintenance schedules for patching and system updates?
- What are the specific details for monitoring and SIEM integration, including alerting?

8. Cost Management

- Azure Cost Management:
- Tagging for cost allocation.
- Budgets and alerts for resource groups and workloads.
- Optimization via Azure Advisor and Reserved Instances.

Departmental Input Required:

- What are the specific cost management requirements, including chargeback/showback models?
- What are the tagging standards that must be enforced for resource groups and resources?

13 Implementation Approach

- Phased Rollout:

2. Deploy foundational elements (management groups, policies, identity, network, security baseline) via IaC.
3. Deploy and test landing zones for each workload type.
4. Migrate workloads in prioritized waves.

Optimize, monitor, and iterate.

> .

14 Plan

This section contains the plan for delivery of the project component including the high-level implementation plan, end-user impact (if applicable) and deployment plans for Azure Cloud Foundation.

14.1 Planning Decisions

The following table documents the planning decisions that have been made for this solution component, including the reasoning for those decisions where applicable:

Category	Topic	Decision	Reasoning
TBC	TBC	TBC	TBC

Table 5 – Planning Decisions

14.2 Implementation Plan

The following is the high-level plan for implementation of the Azure Cloud Foundation design described in this document as part of the interim approach:

- Deploy additional Hubs in AUCentral2 and AUEast regions

Appendix A – Glossary of Terms

Name	Description
AAD	Azure Active Directory
ACL	Access Control List
ACR	Azure Container Resource
AD	Active Directory
ARM	Azure Resource Manager
AV	Anti-Virus
CDC	Canberra Data Centres Pty Ltd
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSC	PowerShell Desired State Configuration
Enrolment	Overarching structure within which all Azure consumption occurs
EP	Endpoint Protection
JSON	A JavaScript Object Notation (JSON) file that defines one or more resources to deploy to a resource group.
NSG	Azure Network Security Group
RBAC	Role-Based Access Control
RG	Azure Resource Group
SN	Azure Virtual Network Subnet
SOE	Standard Operating Environment
URL	Uniform Resource Locator
VM	Virtual Machine
VMSS	Virtual Machine Scale Set

Name	Description
VNet	Azure Virtual Network

Table 6 – Acronyms and Definitions

Appendix B – Requirements

The following list of requirements have been captured by DITRDCA and provided to Microsoft prior to the ACF engagement therefore, these are listed for reference purposes as follows:

Category Name	Description of Requirement
Network	Establish connectivity and integration between the cloud platform and the DITRDCA Protected Network (DPN)
	Supervise connectivity between the CSP environment and DITRDCA
	Network segmentation capability in the projects cloud platform
	Implement network segmentation/segregation (e.g. virtual subnets, gateways/firewalls) required to meet DITRDCA accreditation
Identity and Access Management	Policy that ensures DITRDCA information is only accessible by authorised personnel with; an appropriate level of clearance, a demonstrated need-to-know, and the number of privileged users is kept to a minimum, regularly reviewed and are only assigned the minimum amount of privileges required to perform their assigned tasks.
	Define Directory Service strategy supporting DITRDCA users, cloud resources, applications
	Enable authentication of DITRDCA systems on the DPN, including Active Directory and ICT systems
	Define identity strategy and enable authentication on the DPN
	Provide demonstrated capability and policy in all official information will be safeguarded to ensure its confidentiality, integrity, and availability.
Security Accreditation	Confirmation that all patterns and designs meet security requirements
	Determine security requirements (including definition of encryption and integrity requirements to apply to DITRDCA data at rest and in motion)
	Create and maintain security policies and technical standards
	Determine security strategy and implementation plans; request audit reports
	Definition, review and audit of roles, profiles, authorisations

Category Name	Description of Requirement
	Ability to support, accommodate and record information exchanges across security zones (Unclassified, Protected, Secret) and different DPN domains
	Ability to proactively support CIOG Security Certification/Accreditation activities and ongoing service compliance.
	Establish adequate Security Controls and Operational Monitoring (incl. Encryption)
	The Foundation Platform must be DITRDCA Accredited at the Protected level
	Demonstrated ability to manage cyber security events and cloud forensics in alignment to practices required for DITRDCA accreditation.
	Confirm cloud service provider has been awarded Australian Cyber Security Center (ACSC) Certification and are listed on the Certified Cloud Services List (CCSL).
Implementation	Monitoring, management and reporting capabilities of active workloads, as well as the provider platform itself
	Policy to administer risk management, visibility, accountability, separation of duties and future plans for the cloud service.
Billing	Develop Enterprise Account Management and Procurement patterns as well as report on DITRDCA current footprint with CSP
	Improved traceability to provide real-time and historic reporting for billing, utilisation, availability, performance, usage reports, incidents based on DITRDCA defined metadata tags.
	Demonstrate financial position, pricing transparency and funding models associated with its service and ongoing consumption of its services and provided enough information to allow DITRDCA to assess financial risk
Workload	Demonstration of implementation via workload simulation

Table 7 – Existing DITRDCA Requirements

15 Appendix C – URLs for Whitelisting

The following list of URLs are required for whitelisting within the customers internet proxy environment when communicating with Azure Public cloud:

Name	URL
Azure Portal (Port 80 and 443)	Portal.azure.com Management.azure.com *.aadcdn.microsoftonline-p.com *.aka.ms *.applicationinsights.io *.azure.com *.azure.net *.azureafd.net *.azure-api.net *.azuredatalakestore.net *.azureedge.net *.loganalytics.io *.microsoft.com *.microsoftonline.com *.microsoftonline-p.com *.msauth.net *.msftauth.net *.trafficmanager.net *.visualstudio.com *.windows.net *.windows-int.net
Azure Active Directory (Port 443)	Login.microsoftonline.com *.onmicrosoft.com
Azure App Services (WebApp)	*.azurewebsites.net
Azure Key Vault	Vault.azure.net

Name	URL
(Port 443)	
Azure Storage	*.blob.core.windows.net *.queue.core.windows.net *.table.core.windows.net *.file.core.windows.net
Azure SQL	*.database.windows.net
Azure KMS Service	Kms.core.windows.net:1688 (23.102.135.246/32)
Azure Automation - Update Management (Port 443)	*.ods.opinsights.azure.com *.oms.opinsights.azure.com *.blob.core.windows.net *.azure-automation.net

Table 8 – URLs for Whitelisting

Appendix D – DITRDCA Service Classes

The table below provides the CP service class summary from the DITRDCA FPS document:

Service Management	Class 1	Class 2	Class 3	Class 4	Class 5
Description	High Availability	Critical	Important	Standard	Basic
Common Use	Provides the highest level of service with maximum fault tolerance. Application must provide equal fault tolerance capability. Business justification is mandatory to support this Premium Service Class.	Provides critical level of fault tolerance. Business justification is mandatory to support this Premium Service Class.	Current DITRDCA Production ERP systems (MILIS, Roman, PMKeyS) operate under this Service Class.	Potential use cases are environments which are not business critical but require a minimal DR capability.	Current DITRDCA DEV, TEST, and UAT environments operate under this Service Class.
Support Hours	24 x 7 x 365	24 x 7 x 365	24 x 7 x 365	Business Hours	Business Hours
Availability	0.9999	0.999	0.99	0.98	0.9
Operational RTO	5 mins	< 1 hr	< 24 hours	< 7 Days	4 + weeks

Table 9 – DITRDCA IOC Service Classes