Statement of Work



Cloud Enablement with Azure

Prepared for

**Department of Immigration and Border Protection**

22nd June 2016

Version 1.0

Prepared by

**Leah Owen**

Account Delivery Executive

Leah.Owen@microsoft.com

Table of Contents

[Introduction 5](#_Toc454262745)

[1 Project Objectives and Scope 6](#_Toc454262746)

[1.1 Objectives 6](#_Toc454262747)

[1.2 Areas Within Scope 6](#_Toc454262748)

[1.2.1 General Project Scope 6](#_Toc454262749)

[1.2.2 Software Products / Technologies 7](#_Toc454262750)

[1.2.3 Integration and Interfaces 7](#_Toc454262751)

[1.2.4 Environments 7](#_Toc454262752)

[1.2.5 Training and Knowledge Transfer 8](#_Toc454262753)

[1.2.6 Testing 8](#_Toc454262754)

[1.3 Areas Out of Scope 8](#_Toc454262755)

[2 Project Approach, Timeline, and Service Deliverables 10](#_Toc454262756)

[2.1 Approach 10](#_Toc454262757)

[2.1.1 Cloud Infrastructure Planning and Evaluation 10](#_Toc454262758)

[2.2 Timeline 18](#_Toc454262759)

[2.3 Key Service Deliverables and Acceptance Process 18](#_Toc454262760)

[2.3.1 Key Project Service Deliverables 18](#_Toc454262761)

[2.3.2 Service Deliverable Acceptance Process 19](#_Toc454262762)

[2.4 Project Governance Approach 20](#_Toc454262763)

[2.4.1 Communication Plan 20](#_Toc454262764)

[2.4.2 Issue/Risk Management Procedure 20](#_Toc454262765)

[2.4.3 Change Management Process 21](#_Toc454262766)

[2.4.4 Escalation Process 22](#_Toc454262767)

[2.5 Project Completion 22](#_Toc454262768)

[3 Project Organisation and Staffing 23](#_Toc454262769)

[3.1 Project Organisation Structure 23](#_Toc454262770)

[3.2 Project Roles and Responsibilities 24](#_Toc454262771)

[3.2.1 DIBP Project Roles and Responsibilities 24](#_Toc454262772)

[3.2.2 Microsoft Project Roles and Responsibilities 24](#_Toc454262773)

[4 General Customer Responsibilities and Project Assumptions 26](#_Toc454262774)

[4.1 General Customer Responsibilities 26](#_Toc454262775)

[4.2 Project Assumptions 27](#_Toc454262776)

# Introduction

This Statement of Work (SOW) and any exhibits, appendices, schedules, and attachments to it are made pursuant to the Work Order No. 7-KVJMWLIDD, dated 22nd June 2016, the terms of which are incorporated herein by reference, by and between Department of Immigration and Border Protection (“Customer”, “you”, “your”) and Microsoft Corporation (“Microsoft”, “us”, “we”, “our”) or Microsoft’s affiliate, and sets forth the services to be performed by us related to the Department of Immigration and Border Protection’s (DIBP) Hybrid Cloud Enablement (“project”). This SOW, together with the Work Order, represents the complete baseline for scope, services, service deliverables, and acceptance applicable to this project. All changes to this document will be managed in accordance with the Change Management Process defined within. Any terms not otherwise defined herein will assume the meanings set forth in the Work Order.

This SOW and the associated Work Order expire 30 June 2016, unless they have been formally extended in writing by Microsoft.

The Department of Immigration and Border Protection’s (DIBP) current IT Strategy includes several goals around cloud adoption, agility and service delivery enhancements. DIBP is seeking to explore and document a hybrid cloud design that will assist them to deliver to these goals. Microsoft Azure offers a range of capabilities and services to enable a hybrid cloud platform. DIBP has engaged Microsoft Consulting Services to assist with the planning and design of a hybrid cloud architecture using Azure.

1. Project Objectives and Scope
   1. Objectives

The objective of this project is to assist DIBP plan, design and start implementation of cloud utilizing of Azure with the DIBP environment. The project will achieve this by identifying the core management and supporting capabilities required, then begin to introduce operational frameworks.

* 1. Areas Within Scope
     1. General Project Scope

Microsoft will assist with the planning and integration of Azure into the DIBP environment via the following services:

Table 1: General Project Scope

|  |  |
| --- | --- |
| Work Stream | Scope Description |
| **Cloud Design and Implementation** | Conduct a series of planning and evaluation workshops with DIBP on Microsoft Azure and the capabilities required for establishing a cloud enabled architecture. The workshops will cover the core capabilities including Azure Services, Deployment and Configuration, Security and Identity, Connectivity, Management Services, Charge-back and selected cloud workloads.  Develop a High Level Design for the ‘DIBP Hybrid Cloud’ with Azure.  Implement agreed components of the design which will include Azure Active Directory, the designed Subscription/User Roles Model, Consumption Reporting and a VPN accessible IaaS environment for Development. |
| **Azure Resource Manager (ARM) Template Authoring Planning and Development** | Conduct a planning and evaluation workshop with DIBP on Azure Resource Manager including an overview of core Azure Resource Manager (ARM) concepts, APIs and developing Azure Resource Manager (ARM) templates for provisioning.  Lead hands-on planning and development activities around the deployment of one sample and one custom ARM template deployment. |
| **Azure Operations Planning** | Conduct a planning and evaluation workshop with DIBP to define an Azure operations framework including:   * Azure service delivery * Service integration for hybrid cloud delivery * Define roles and responsibilities * Azure operational guidance |
| **Azure Adoption Planning (Cloud Adoption Framework)** | Overview of the tools, services, templates, and guidance needed to transition customers from their current state to the long-term cloud vision aligned with their organisational goals, divided into clear phases:   * Cloud Strategy * Adoption Planning * Adoption |

* + 1. Software Products / Technologies

The products listed in the table below are required to deliver this project. DIBP is responsible for obtaining all required licenses and products.

Table 3: Software Products/Technologies Required

|  |  |
| --- | --- |
| Product/Technology Item | Required By |
| Supported Windows Server 2012 Hyper-V hardware environment (development environment, able to connect to Azure services) | Project start |
| Microsoft Azure subscription | Project start |

* + 1. Integration and Interfaces

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

To explore and implement cloud scenarios, the on-premises Windows Server 2012 environment requires integration with Azure Active Directory (Azure AD). DIBP must have a valid Microsoft Azure AD account that is the directory administrator for at least one Azure Active Directory. This Azure AD account is used as the service administrator account for the environment. The service administrator can configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In the portal, they can create website clouds, virtual machine private clouds, create plans, and manage user subscriptions.

No other integration or interfaces are included in the scope of this Statement of Work.

* + 1. Environments

The following environments are included in the scope of this Statement of Work. The target environment must include an on-premises supported Windows Server 2012 hardware environment.

Table 2: Required Environments

|  |  |  |  |
| --- | --- | --- | --- |
| Environment | Location | Responsibility | Ready By |
| Standalone (Development) | On DIBP premises | Customer | Within one week of project start date |
| Microsoft Azure Subscription | DIBP selected Microsoft Azure Region | Customer | Within one week of project start date |

* + 1. Training and Knowledge Transfer

No formal training is included in the scope of this Statement of Work.

Informal knowledge transfer will be provided throughout the project and during the scope of the project during project collaboration. Informal knowledge transfer is defined as customer’s staff working alongside Microsoft staff.

* + 1. Testing

There will be no formal testing as part of this Statement of Work. Implementation effort will be provided to inform design, support DIBP implementation, and assist with knowledge transfer to DIBP technical resources and key stakeholders.

* 1. Areas Out of Scope

Any area that is not explicitly listed in Section 1.2 as “within scope” is out of scope for this engagement. The areas that are out of scope for this engagement include, but are not limited to, the following:

* Installation of hardware (racks, servers, etc.) or sourcing or procurement of hardware and/or software.
* Custom setup of the on-premises environment, including hypervisors, management hosts, or configuration of the fabric.
* Integration of existing customer, Microsoft, third-party and in-house developed products, components or other solutions outside of those defined in this statement of work.
* Workload application compatibility, custom application remediation or configuration or integration of workloads, Microsoft or 3rd party.
* Building and conducting end-user training classes and materials including certification or accreditation activities.
* Operating or maintaining DIBP’s systems.
* Detailed design and formal review of Project Work Products.
* Development of DIBP’s operational processes and service level agreements.
* Setup or configuration of any other environments outside of those defined in this statement of work.
* Setup of the Azure Subscription. Microsoft will provide guidance and support as part of the work, but customer IT staff will be responsible for Azure setup and configuration.
* Azure subscriptions. Customer is responsible for acquiring all necessary subscriptions required as a result of Work Order.
* Microsoft Azure Stack installation or configuration.
* Source code review. DIBP will not provide Microsoft with access to non-Microsoft source code or source code information. For any non-Microsoft code, Microsoft’s services will be limited to analysis of binary data only, such as a process dump or network monitor trace.

1. Project Approach, Timeline, and Service Deliverables
   1. Approach

Microsoft will leverage the Microsoft Solutions Framework (MSF) to deliver this Statement of Work. MSF represents an industry-proven solution development approach providing well-defined phases that address development of requirements, architectural design, detailed software design, software development, system testing, and managed release cycles. MSF organises the solution approach into five distinct phases during the project lifecycle.

* **Envision**: Envisioning involves creating a business vision and defining the scope of work necessary to bring the vision to reality
* **Plan**: Planning continues through the development of detailed functional requirements, system and application architectures, the user interface prototype, and a detailed project plan for the remainder of the project
* **Build**: The Build phase begins with the first iteration of development and culminates with the “functionality complete” milestone (or Beta release)
* **Stabilise**: The Stabilisation phase involves testing and acceptance
  + 1. Cloud Infrastructure Planning and Evaluation
       1. Envision

##### Key Microsoft Activities

Table 3: Microsoft Activities: Envisioning Phase

|  |  |  |
| --- | --- | --- |
| Activity | Description | Details |
| Envisioning  (time-boxed to 2 days) | Conduct solution overview for awareness of capabilities and options to determine mutually agreed-upon scenarios for initial planning and evaluation | Microsoft will lead one half day session to provide an overview of the project, its goals and assist in preparing prerequisites and dependencies. |

##### Key Customer Activities

Table 4: Key Customer Activities

|  |  |
| --- | --- |
| Activity | Description |
| Validated infrastructure is available and configured | Verify that the required virtualisation environment has been deployed and is available prior to the start of the project |
| Identify key participants (management and subject matter specialists) for envisioning | Confirm key personnel are identified to confirm all stakeholders are represented during the envisioning process |
| Key participants attend envisioning meetings to provide input and drive vision/scope | Confirm key personnel are available and engaged in the envisioning process |
| Validated Internet, Microsoft Azure Active Directory environment is in place and network and firewall access is configured. | Verify that the DIBP datacenter is properly connected to Microsoft Azure Active Directory. |

##### Key Work Products and Deliverables (Microsoft)

*Table 5: Key Work Products and Deliverables (Microsoft)*

|  |  |
| --- | --- |
| Key Work Products and Deliverables (Microsoft) | Description |
| Vision/Scope | Vision/Scope Document including the overall scope of the project work including future project goals and objectives. This document also includes the business opportunity and current environment analysis. |

##### Key Phase Assumptions

Table 6: Key Phase Assumptions

|  |
| --- |
| Key Phase Assumptions |
| Full participation in the envisioning and requirements gathering by Customer decision makers, architects, and subject matter specialists since the effort is short in duration |
| Customer participants in the workshops are empowered to make final decisions during vision/scope development |

* + - 1. Plan

##### Key Microsoft Activities

Table 7: Microsoft Activities: Planning Phase

|  |  |  |
| --- | --- | --- |
| Work Stream | Activity | Details |
| Cloud Design and Implementation  (time-boxed to 10 days) | Conduct a series of design and evaluation workshops with DIBP on Azure and the required capabilities required for establishing a Hybrid architecture. | High Level Solution Design Document covering:   * Services Catalogue Descriptions of Hybrid/Azure based Services * Key Design Decisions * Logical and Physical Designs * Security Design * Identity Design * Management Components * Approach to Charge-back |
| Azure Resource Manager (ARM) Template Authoring Planning and Development  (time-boxed to 3 days) | Conduct a design and evaluation workshop with DIBP on Azure Resource Manager template authoring, | Solution Alignment Workshop covering:   * ARM Overview and Vision * ARM Concepts * Authoring ARM Templates * ARM Template Features * ARM Template Security * ARM Template Best Practices |
| Review and develop ARM template specification. | Review Azure-compatible Microsoft-provided application sample  Review Azure-compatible customer-provided application  Develop high-level ARM Template Specification (deployment process workflow and dependent components) |
| Azure Operations Planning  (time-boxed to 3 days) | Conduct a planning and evaluation workshop with DIBP on Azure Operations. | Solution Alignment Workshop covering:   * Azure Service(s) map overview * Azure Service(s) description * Azure Service integration guidance * Azure Service broker guidance * Azure RACI * Azure role and operational guidance |
| Azure Adoption Planning (Cloud Adoption Framework)  (time-boxed to 5 days) | Conduct a planning workshop with DIBP on Azure cloud adoption. | Overview of the Cloud Adoption Framework which provides the tools, services, templates, and guidance needed to transition DIBP from their current state to the long-term cloud vision aligned with their cloud adoption goals. The modules and topics covered in the workshop include:   * Cloud Adoption Framework Foundation * Cloud Adoption Strategy * Cloud Adoption Planning * Cloud Security * Data Governance * Cloud Service Broker |
| Create a cloud adoption plan with DIBP for Azure | Initiative Discovery Co-Creation   * High-level initiative discovery performed at workshop as co-creation effort   Adoption Plan   * Formal adoption plan created outside of workshop utilising output of the previous workshop |

##### Key Customer Activities

Table 8: Key Customer Activities

|  |  |
| --- | --- |
| Activity | Description |
| Identify key participants (management and subject matter professionals) for design discussions. | Confirm key personnel are identified to confirm all stakeholders are represented during the design workshops and discussions. |
| Key participants attend planning meetings to provide input and drive functional specification refinement | Confirm key personnel are available and engaged in the requirements gathering process. |
| Identify Candidate Application for ARM Template Development | Identify a single, compatible/qualified application that can be transformed into a ARM template within the scope of the engagement (overall ARM template workshop (effort is time-boxed to 5 days). |
| Assist with the identification and validation of pre-requisites | Confirm key personnel from each application workload that will be used in the Proof of Concept are available and actively participating in the discovery and rationalisation process. |

##### Key Work Products and Deliverables (Microsoft)

Table 9: Key Documents/Objectives (Microsoft)

|  |  |
| --- | --- |
| Key Work Products and Deliverables (Microsoft) | Description |
| High Level Design (HLD) | HLD for the implementation of a Hybrid Cloud Solution utilising Azure. |
| Assist with the Adoption Plan | High-level adoption plan document created outside of workshop utilising output of the previous workshop. |

##### Key Phase Assumptions

Table 10: Key Phase Assumptions

|  |
| --- |
| Key Phase Assumptions |
| Full participation in the requirements gathering by DIBP decision makers, architects, and subject matter specialists. |
| Customer provides application server access for systems agreed to during the Solution Alignment Workshop before moving to the build phase. |

* + - 1. Build

##### Key Microsoft Activities

Table 11: Microsoft Activities: Build Phase

|  |  |  |
| --- | --- | --- |
| Work Stream | Activity | Details |
| Cloud Design and Implementation  (time-boxed to 13 days) | Build core components included in the High Level Design to enable Cloud capability. | * Configure Azure Active Directory Synchronisation * Configure System Center Configuration Manager, Service Manager, Operations Manager and PowerShell scripting * Configure Subscriptions, roles and permissions with consumption reporting and emailed threshold notifications * Assist configure connectivity in Azure to allow DIBP access. Provide guidance on DIBP connectivity to Azure |
| Azure Resource Manager (ARM) Template Authoring Planning and Development  (time-boxed to 5 days) | Development of ARM Template Samples | * Configure Visual Studio, load sample templates, demonstration of the applicable features * Develop Sample Azure Resource Manager template (based on Microsoft Provided sample) * Develop Sample Azure Resource Manager template (based on specification) * Develop ARM Template Publishing Plan (.json, Portal, PowerShell and required RBAC roles) |
| Azure Operations Planning  (time-boxed to 2 days) | Review and Development of Sample Azure Operations Plan Artifacts | * Review Sample Service Map * Review Sample Service Description * Review Sample Service Integration Checklist * Review Service Broker Function * Review Sample Azure IaaS RACI Chart * Review Sample Azure IaaS Operational Tasks * Review Sample Azure IaaS Role Guidance |

##### Key Customer Activities

Table 12: Key Customer Activities

|  |  |
| --- | --- |
| Activity | Description |
| Identify key participants (management and subject matter professionals) for system integration | Confirm key personnel are identified to confirm deployment times are reduced |
| Change Management | Change management approvals |
| Perform onsite hardware/virtualised system installation and configuration | Actively assist in the onsite hardware and virtualised system installation and provide Hyper-V administrative access as required |
| Complete all assigned actions by the agreed due dates. | N/A |

##### Key Work Products and Deliverables (Microsoft)

Table 13: Key Documents/Objectives (Microsoft)

|  |  |
| --- | --- |
| Key Work Products and Deliverables (Microsoft) | Description |
| Assist with the deployment of all required systems | Provisioning and assistance with the configuration of the Development and Azure environments |

##### Key Work Products and Deliverables (Customer)

*Table 14: Key Work Products and Deliverables (Customer)*

|  |  |
| --- | --- |
| Key Work Products and Deliverables (Customer) | Description |
| Assist with the deployment of all required systems | Assist with the deployment of demonstration workloads and on premises capabilities. |
| Change Management Approvals | Manage the DIBP change control process |

##### Key Phase Assumptions

Table 15: Key Phase Assumptions

|  |
| --- |
| Key Phase Assumptions |
| Full participation by Customer decision makers, architects, and subject matter specialists for hardware and virtualisation infrastructure deployment |
| Hardware integration will be performed by the Customer prior to the architecture implementation in the lab environment |

* + - 1. Stabilise

##### Key Microsoft Activities

Table 16: Microsoft Activities: Stabilise Phase

|  |  |  |
| --- | --- | --- |
| Activity | Description | Details |
| Cloud Design and Implementation  (time-boxed to 5 days) | Conduct demonstrations and review workshops to generate design updates and future project planning for DIBP | Conduct a demonstration of the enabled cloud features implemented on premises and in Azure  Review the built capability against the Vision/Scope document provided in the Envisage Phase (both targeted outcomes for the project and future goals for DIBP)  Update the Vision/Scope and Hybrid Cloud High Level Design Documents with outcomes from the review |
| Azure Resource Manager (ARM) Template Authoring Planning and Development  (time-boxed to 2 days) | Validation of functionality and high-level documentation of the developed ARM template | Review Customer-provided Application Azure ARM Template (based on specification)  Update documentation of the ARM deployment template and dependent components as required |

##### Key Work Products and Deliverables (Microsoft)

Table 17: Key Documents/Objectives (Microsoft)

|  |  |
| --- | --- |
| Key Work Products and Deliverables (Microsoft) | Description |
| Review Hybrid Cloud build and Azure Resource Manager Templates with DIBP | Update documentation as required |

##### Key Work Products and Deliverables (Customer)

*Table 18: Key Work Products and Deliverables (Customer)*

|  |  |
| --- | --- |
| Key Work Products and Deliverables (Customer) | Description |
| Coordinate resources for demonstrations and review against Vision/Scope | Coordinate resources for demonstrations and reviews  Facilitate any necessary communication or information for reviews/feedback  Work with Microsoft to identify project the team members  Make decisions where architectural options are presented |
| Engage and communicate support strategy, procedures, and information necessary for your Help Desk and field technical support | Identify and communicate the support strategy within the organisation |
| Submit and obtain approvals for all customer change control processes required for production deployment in subsequent phases | Manage the DIBP change control process |

##### Key Phase Assumptions

Table 19: Key Phase Assumptions

|  |
| --- |
| Key Phase Assumptions |
| Customer will coordinate all resources and communicate the support plan |

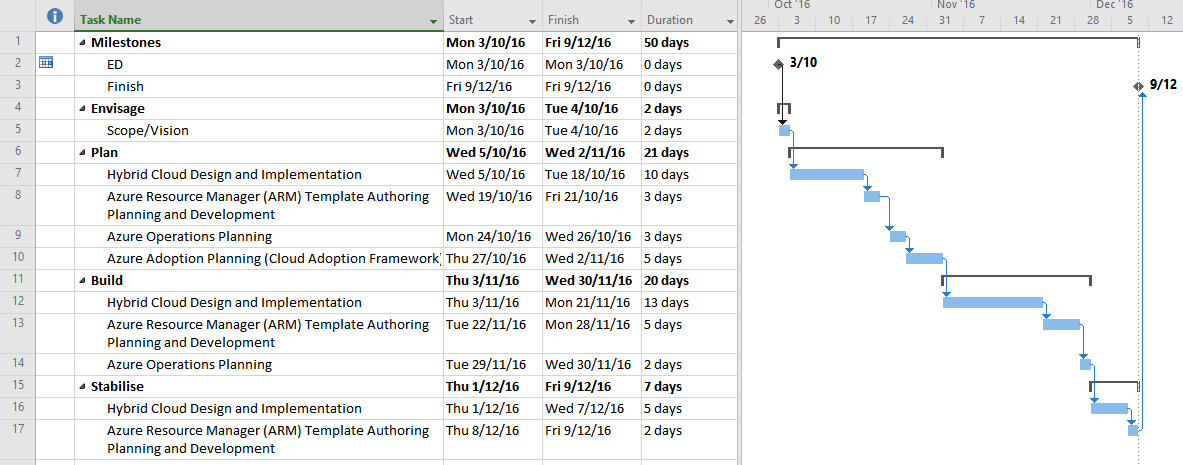
* 1. Timeline

It is estimated that this engagement will be performed over a period of 8 weeks and will include the phases noted. The actual timeline for this engagement will be relative to the project start date, and all dates and durations provided are estimates only.

Please note;

* Holidays, vacation, and training time have not been factored into this Statement of Work.
* All work is to be contiguously scheduled.
* The standard work week for the project will be Monday through Friday, except for scheduled holidays.
* The schedule is dependent upon customer dependencies also being achieved on time.

Table 20: Engagement deliverables



* 1. Key Service Deliverables and Acceptance Process
     1. Key Project Service Deliverables

The following is a list of the key project Service Deliverables that will be produced within the scope of this SOW and which must be formally reviewed and accepted under the process described below.

Table 21: Key Project Service Deliverables

|  |  |  |
| --- | --- | --- |
| Project Phase | Service Deliverable Name | Service Deliverable Descriptions |
| Envision | Vision/Scope document | Outline of the customer goals for the project, in scope and out-of-scope areas of the project as well as documented requirements, and constraints for the Microsoft Azure Site Recovery Service |
| Plan | High Level Design (HLD) Document | HLD for Cloud implementation with Azure |
| Stabilise | Azure Resource Manager template high-level document | Documented summary of the developed ARM template |

* + 1. Service Deliverable Acceptance Process

At specified milestones throughout the project, Microsoft will submit completed project Service Deliverables for Customer’s review and approval. Service Deliverables will fall into the following categories:

1. Document Deliverables (e.g. Word, Excel, Visio, Project, etc.)
2. Functioning Components or Solution Deliverables (e.g. custom source code)

Customer’s use or partial use of a Service Deliverable will constitute acceptance of that Service Deliverable. Customer may provide its acceptance and/or rejection of deliverables electronically via email. The following details the acceptance process for each of the deliverable types.

***Document Deliverables:*** Within 5 business days from the date of submittal, customer must either

1. accept the Document Deliverable by signing, dating, and returning the Service Deliverable Acceptance Form, or
2. provide a written notice rejecting the Document Deliverable, including a single and complete list describing every reason for rejection.

Document Deliverables shall be deemed accepted unless Customer provides a timely, written rejection notice as described above.

Microsoft will correct problems with a Document Deliverable that are identified in the written rejection notice, as described above, and within the scope of this Statement of Work, after which the Document Deliverable will be deemed accepted.

Issues that are outside the scope of this Statement of Work and feedback provided after a Document Deliverable has been deemed accepted will be addressed as a potential change of scope pursuant to the Change Management process outlined in this SOW.

***Functioning Components or Solution Deliverable(s):*** The functioning solution is typically comprised of configured commercial software and custom source code and associated objects. Review and acceptance of the solution or custom source code, for this SOW only, is based on completion / sign off of the defined Customer Acceptance Test.

* 1. Project Governance Approach

The project will be managed by the Microsoft Project Manager. Prior to the start of the engagement, a mutually agreed to coverage plan / meeting schedule will be documented in writing. As this resource is part-time, the following operational constraints are assumed:

Table 22: Project Management Activities

|  |  |
| --- | --- |
| Project Management | Description |
| Communications | Provide 1 weekly status Report. Prepare and lead 1 status meeting per week of no more than 1 hour in duration. Note: All customer meetings will NOT be attended. |
| Scope Management / Change Control | Attend 1 Scope meeting. Manage project Change Control. |
| Finance | Provide weekly Budget Report as part of the weekly status report. |
| Schedule | Manage the schedule for the Microsoft scope of work and Microsoft resources. |
| Human Resources / Staff Management | Coordinates Microsoft resources (only), including staffing, task assignments and status reporting. |

Microsoft will provide project management for the duration defined in the Work Order. Changes to this duration or the amount of hours per week will be handled by the Change Management Process.

* + 1. Communication Plan

The following will be used to provide formal communication during the course of the project:

* The Microsoft Project Manager, working in conjunction with the Customer Project Manager, will document a detailed Communication Plan as part of the Master Project Management Plan
* The Microsoft Project Manager, working in conjunction with the Customer Project Manager, will compile weekly status reports for distribution to both Customer and Microsoft management
* Weekly status meetings will be held to review the project’s overall status, the acceptance of deliverables, the project schedule, and open issues noted in the status report
  + 1. Issue/Risk Management Procedure

The following general procedure will be used to manage active project issues and risks during the project:

* **Identify:** Identify and document project issues (current problems) and risks (potential events that impact the project)
* **Analyse & Prioritise:** Assess the impact and determine the highest priority risks and issues that will be managed actively
* **Plan & Schedule:** Decide how high-priority risks are to be managed and assign responsibility for risk management and issue resolution
* **Track & Report:** Monitor and report the status of risks and issues and communicate issue resolutions
* **Control:** Review the effectiveness of the risk and issue management actions

Active issues and risks will be monitored and reassessed on a weekly basis. Mutually agreed upon issue escalation and risk management processes will be defined at the outset of the project.

* + 1. Change Management Process

During the project, either party may request, in writing, additions, deletions, or modifications to the services described in this SOW (“change request”).

For all change requests, regardless of origin, Microsoft shall submit to Customer Microsoft’s standard Change Request Form, which shall describe the proposed change(s) to the project, including the impact of the change(s) on the project scope, schedule, fees, and expenses.

For all change requests which Customer originates, Microsoft shall have a minimum of 3 business days from receipt of the change request to research and document the proposed change, and prepare the Change Request Form.

Customer shall have 3 business days from your receipt of a completed Change Request Form to accept the proposed change(s) by signing and returning the Change Request Form. If Customer does not sign and return the Change Request Form within the time period prescribed above, the change request will be deemed rejected and Microsoft will not perform the proposed change(s).

No change to this project shall be made unless it is requested and accepted in accordance with the process described in this section. Microsoft shall have no obligation to perform or commence work in connection with any proposed change until a Change Request Form is approved and signed by the designated Project Managers from both parties.

At Microsoft’s discretion, time required to research and document customer originated change requests will be billed at the standard rates specified in the project Work Order.

* + 1. Escalation Process

The Microsoft Project Manager will work closely with the Customer Project Manager, Sponsor, and other designees to manage Project issues, risks, and Change Requests, as described in Sections 2.4.2 and 2.4.3 above. The standard escalation process for review and approval and/or dispute resolution is as follows:

* + - 1. Escalation Path
* Project Team member (Microsoft or Customer)
* Microsoft Delivery Manager / DIBP Program Manager
* Microsoft Account Delivery Executive / DIBP Executive Project Sponsor
  1. Project Completion

The project will be considered complete when any of the following conditions is met:

1. All of the service deliverables identified within this SOW and any Change Requests accepted pursuant to the Change Management Process defined in this document, delivered and accepted or deemed accepted; or
2. The fee provisions of the Work Order have been met; or
3. This SOW is terminated pursuant to the provisions of the agreement.
4. Project Organisation and Staffing
   1. Project Organisation Structure

This section describes the overall project organisation structure, reporting relationships, and key project roles.

The project will be organised as depicted in the following diagram.



Figure 1: Project organisation structure

* 1. Project Roles and Responsibilities

This section provides a brief description of key project roles and responsibilities.

* + 1. DIBP Project Roles and Responsibilities

Table 23: DIBP roles and responsibilities

|  |  |
| --- | --- |
| Role | Responsibilities |
| DIBP Executive Sponsor | Executive Sponsorship and alignment with DIBP strategy |
| DIBP Program Manager | Assists in escalating unresolved issues and clears project roadblocks |
| DIBP Project Manager | Primary point of contact for Microsoft team  Responsible for managing and coordinating the overall project  Responsible for resource allocation, risk management, project priorities, and communication to executive management  Manages day-to-day activities of the project  Coordinates the activities of the team to deliver deliverables according to the project schedule |
| DIBP Technical Team Lead | Primary point of contact for technical activities by team members below  Coordinates installation and configuration activities for all required hardware elements  Primary technical point of contact for the team that is responsible for technical architecture and planning |
| DIBP App Workload Lead | Primary point of contact for app specific questions and activities (for ARM template authoring) |
| DIBP Network Lead | Primary point of contact for managing and performing the configuration of all network related activities |
| DIBP Storage Lead | Primary point of contact for storage decisions and configuration activities |
| DIBP Active Directory Lead | Primary point of contact for Azure Active Directory decisions and configuration activities |
| DIBP Security Lead | Primary point of contact for any required Security approvals or considerations |

* + 1. Microsoft Project Roles and Responsibilities

Table 24: Microsoft roles and responsibilities

|  |  |
| --- | --- |
| Role | Responsibilities |
| Microsoft Account Delivery Executive | Microsoft’s escalation point and accountable for overall DIBP program delivery strategy and excellence. |
| Microsoft Service Delivery Manager | Responsible for deliverable quality and DIBP’s overall satisfaction with Microsoft’s services  Single point of contact for billing issues, personnel matters and contract extensions |
| Microsoft Project Manager | Project management of Microsoft deliverables and resources  Stakeholder management  Responsible for Microsoft resource allocation, risk management, project priorities, and communications |
| Microsoft Lead Architect | Responsible for overall solution design  Provide technical oversight  Verifies whether Microsoft recommended practices are followed  Gather and assemble all project management plans, project status reports, and project performance reports  Responsible for managing and coordinating the overall Microsoft project  Manages day-to-day activities of project  Coordinates the activities of the team to deliver deliverables according to the project schedule  Responsible for delivering the Cloud Adoption Framework workshop |
| Microsoft Azure Consultant | Responsible for the delivery of on premises and Azure documentation, implementations and reviews |

1. General Customer Responsibilities and Project Assumptions
   1. General Customer Responsibilities

Delivery of Microsoft’s services depends upon, among other things, the following:

* DIBP’s involvement in all aspects of the services.
* DIBP’s ability to provide accurate and complete information, as needed.
* DIBP’s timely and effective completion of the responsibilities, as identified herein.
* DIBP’s deployment of the selected hardware configuration.
* The accuracy and completeness of the Assumptions, identified below.
* DIBP’s completion of site readiness activities and hardware setup.
* All documents/objectives are accepted at time of delivery by DIBP.
* Throughout the project, Microsoft will submit requests for decisions or feedback for Customer to complete. Decisions are assigned due dates, and it is assumed that Customer will provide the required feedback or make decisions on either the due date agreed upon or (3) business days from the date of submittal. If a decision or feedback is not provided within the due date or (3) business days, it will be addressed as a potential change of scope pursuant to the Change Management process outlined in this SOW.
* Site readiness activities that are a prerequisite for the completion of MCS tasks (e.g., hardware deployment). Failure to complete all site readiness activities that are required for Microsoft to deliver its services according to the agreed upon project schedule may result in project delays requiring Change Orders to this project as well as additional project costs.
* The customer environment will be ready in preparation for the build and deploy phases. DIBP’s existing infrastructure including Active Directory, DNS, network connectivity and other dependent infrastructure is deployed in a supported configuration.
* Product licenses (Microsoft or non-Microsoft) will not be provided as part of this project. You are responsible for acquiring all necessary product licenses or Microsoft Azure subscriptions required as a result of this project.

In addition to any Customer activities identified elsewhere in this SOW, DIBP will perform or provide the following:

* Work with the Microsoft Project Manager to deliver the Project on schedule.
* Manage Project plan(s), schedules, etc.
* Make key day-to-day decisions and provide a single point of contact.
* Manage the Employment Suitability Clearance (ESC) process and onsite access for Microsoft staff.
* Provide personnel who are knowledgeable about the current DIBP systems.
* Provide business user representatives as required by the project plan.
* Provide all personnel needed to conduct the acceptance testing of the solution.
* Provide access to all necessary DIBP work sites, systems logon and passwords.
* Provide access to other materials and resources as needed and as advised by us in advance.
* Provide suitable work spaces with desks, chairs, telephones, etc.
* Provide LAN/WIFI connections giving the Microsoft onsite team access to the Internet.
* If available, provide remote access capabilities to the Microsoft team during delivery.
* Assume responsibility for management of all non-Microsoft managed vendors.
* Provide access with proper licenses to all necessary tools and third party products required for Microsoft to complete its assigned tasks.
* One Microsoft Azure subscriptions for Azure Active Directory integration.

In performing services under this SOW and the applicable Work Order, Microsoft will rely upon any instructions, authorisations, approvals, or other information provided by Customer’s Project Manager or personnel duly designated by Customer’s Project Manager.

* 1. Project Assumptions

There are no project assumptions.