Services Offering Description

XAB-DDS-PP

ONE IDENTITY PASSWORD MANAGER ADVANCED PACKAGE PREPAID EXPERT SERVICE

One Identity typically recommends a phased approach to implementation, which is completely flexible and designed to achieve the most efficient/effective delivery schedule, whilst optimising the transfer of knowledge to customer resources.

One Identity Expert Services have a well-defined project management methodology for deploying Identity and Access Management solutions. The methodology provides governance around our engagement approach which is based on the stages described below.

The tasks will vary depending on the project scope and the One Identity technologies being deployed; however, the stages and engagement approach will remain the same. The following sections provide an overview of each stage, typical tasks, deliverables and resources.

In the activities below, where Configuration Items such as Assets or Users are added, "up to nn" is used to denote the guaranteed amount that the Vendor will commit to creating/onboarding as part of the engagement. The customer's admin teams will be able to complete the remainder (and manage in BAU) using the knowledge they have gained from the Vendor's consultant during the engagement.

CORE FEATURE DELIVERABLES:

The solution provided by One Identity will include:

1. Workshop with customer to verify the pre-requisites for the engagement. [0.5 days]

2. Deployment of One Identity Password Manager components
    a. Up to 2 One Identity Password Manager Service servers
    b. Up to 2 One Identity Password Management Web Interface servers
        i. Configuration to user a customer supplied and configured network load balancer

3. Supply details for Group Policy settings required for Secure Password Extensions

4. Initial configuration, plus product configuration:
    a. Connection to a single AD Domain
    b. Email configuration
    c. General settings
    d. RADIUS or Starling 2FA configuration

e. Backup of configuration
f. Configuration of reporting

5. Configuration of a single Management Policy
    a. User scopes (as defined by a single AD group or an Organizational unit)
    b. Helpdesk scopes (as defined by a single AD group or an Organizational unit)
    c. Question and Answer profile questions (as supplied by the customer, up to a total of 10 questions)
    d. Modifications to workflows to support 2FA

6. Configuration of One Identity Password Manager Password Policy (up to 1)

Deliverables: *Fully commissioned system with the first trial users registered.*

PREREQUISITES AND ASSUMPTIONS

The Activities are based on the following specific assumptions:

The customer has completed all activities required in the Pre-Requisites

1. Deliver phase:
    1.1. The customer has made appropriate administrative and service accounts details available to the consultant performing the engagement.
    1.2. The service accounts used by One Identity Password Manager has enabled, with all the correct permissions as defined in the Pre-Requisites
    1.3. All network and hardware requirements have been met (Firewall's open, servers accessible)
    1.4. Customer has already deployed the Secure Password Extension component to at least 1 workstation/laptop for confirmation of functionality.
    1.5. Customer has already deployed the Password Policy Manager component to all domain controllers within the single AD Domain for confirmation of functionality.