## Hardened Forest Administrative Environment

Statement of Work

Prepared for

Prepared by

Date: February 28, 2020

Version: 1.0



## Table of Contents

[INTRODUCTION 1](#_TOC_250022)

1. [PROJECT OBJECTIVES AND SCOPE 2](#_TOC_250021)
   1. [OBJECTIVES 2](#_TOC_250020)
   2. [AREAS WITHIN SCOPE 2](#_TOC_250019)
      1. [General Project Scope 2](#_TOC_250018)
      2. [Software Products and Technologies 6](#_TOC_250017)
      3. [Data Migration 7](#_TOC_250016)
      4. [Integration and Interfaces 7](#_TOC_250015)
      5. [Environments 8](#_TOC_250014)
      6. [Training and Knowledge Transfer 8](#_TOC_250013)
   3. [AREAS OUT OF SCOPE 8](#_TOC_250012)
2. PROJECT APPROACH, TIMELINE, AND SERVICE OUTCOME 11
   1. [APPROACH 11](#_TOC_250011)
      1. [Envision Phase 11](#_TOC_250010)
      2. [Plan Phase 13](#_TOC_250009)
      3. [Build Phase 15](#_TOC_250008)
      4. [Stabilize Phase 16](#_TOC_250007)
      5. [Deploy Phase 18](#_TOC_250006)
   2. [TIMELINE 20](#_TOC_250005)
3. [PROJECT ORGANIZATION AND STAFFING 21](#_TOC_250004)
   1. [PROJECT ORGANIZATION STRUCTURE 21](#_TOC_250003)
   2. [PROJECT ROLES AND RESPONSIBILITIES 22](#_TOC_250002)
      1. [Customer Project Roles and Responsibilities 22](#_TOC_250001)
      2. [Microsoft Project Roles and Responsibilities 22](#_TOC_250000)

This **‘Hardened Forest Administrative Environment’** Statement of Work (SOW) and any exhibits, appendices, schedules, and attachments to it are made with accordance to the Master SOW (Modern Workplace for Spin-Off). Each chapter in the Master SOW applies to this document.

## Introduction

, like many organizations in both the commercial and government sectors, faces an increasingly challenging cyber threat environment. Attackers have become sophisticated in both attack methodologies and in navigating business/social structures to obtain the information they are seeking. These modern cyber-attackers are adept at rapidly gaining administrative access to computing environments. These attacks are difficult to identify and typically result in remote malicious actors with unfettered access to most or all of an organization’s electronic documents, including emails, reports, presentations, customer data, and other intellectual property. These attackers sometimes also target an organization as a relay point to attack customers, suppliers, employees, or trusted business partners of the organization.

Protecting against these attacks is a key priority for .

This project looks through the lens of a tiered model. Tier 0 is defined as the users, software and hardware that are equivalent in privilege to domain or enterprise administrators or have control over them. Tier 0 represents the highest tier with the highest privilege accounts that have permissions into the lower tiers, namely Tier 1 which is used to house application servers (e.g.

Exchange, SharePoint and SQL) and Tier 2 which houses the standard user workstations.

This project, called Enhanced Security Administrative Environment (HF), only focuses on Tier 0, ensuring the root of the infrastructure is protected and trusted. The other tiers should be addressed in separate projects.

The implementation of HF should be performed together with other mitigations, e.g. drastically reduce the of number of Domain and Enterprise admin account, removal of application services account from Domain Admin group, and Domain Controller hardening in order to increase the overall security posture against credential theft attacks.

# Project Objectives and Scope

This chapter details the project objectives and scope.

## Objectives

The objective of the project is to design and implement the Enhanced Security Administrative Environment HF for Tier-0 accounts (Domain Administrators, Enterprise Administrators, and equivalent), based upon Microsoft-recommended practices, architectures, accumulated field experience, and requirements.

HF helps protect these Tier-0 accounts with dedicated administrative workstations, enhanced security controls and configurations, and a dedicated environment to support and maintain the lifecycle of users and workstations.

## Areas Within Scope

This section details the areas within scope.

### General Project Scope

Microsoft will Support the customer in the following areas:

Table 1: Services in Scope

|  |  |  |  |
| --- | --- | --- | --- |
| **Solution**  **Component** | **In-Scope Feature** | **Description and**  **Considerations** | **Scope Assumptions** |
| HF envisioning | Up to three days of envisioning workshops | Microsoft will provide up to three days of envisioning workshops to define the overall project vision and major design decisions,  captured in the vision and scope document. | Three days of envisioning workshop based on the HF reference architecture. |
| HF design | Detailed logical and physical design of the HF environment | Microsoft will adapt HF reference architecture to fit environment. Detailed design workshops will be scheduled to determine the final HF design. | HF reference architecture is used as a baseline, with specific features and configurations that are mandatory, recommended, or optional.  The baseline scales to up to 20 production DCs.  Environments with more than  20 production DCs require an add-on that will |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | appropriately scale HF solution components. |
| HF  administrative workstation image | Design of a single workstation image | One administrative workstation image for Windows 10 Enterprise x64 is prepared in the Microsoft Deployment  Toolkit (MDT). | One image is in scope. |
| Network traffic security | Planning and configuration of IP security (IPsec) in HF environment | This configuration will facilitate authentication and, if required, encryption of traffic between administrative workstation hosts and managed resources.  Scope includes a purpose-built public key infrastructure (PKI) certification authority (CA) in the HF environment to provide certificates for HF hosts and production DCs. | CA for the issuance of administrative smart cards and IPsec certificates is a required component to help secure communications between the production forests and the administration (HF) forest. |
| Smart card configuration | Design, configuration, and deployment of customer- supplied smart cards for accounts in the solution domain to ’  administrators | HF environment is configured with one type of customer- supplied smart card. | Customer-supplied smart cards must be compatible with the Microsoft Base Smart Card Cryptographic Service Provider standard. |
| Security alerting | Plan and configuration of security alerting in HF using System Center Operations Manager | This capability is also extended to production DCs and requires installation of management agents on production DCs. | Basic operational health monitoring for hosts is in scope, but management pack tuning is not in scope. |
| System testing assistance | Assist with testing of the HF solution items within the non-production build  environment | System testing focuses on the functionality meeting the design. | Testing assistance is constrained to the time allocated during this project. |
| Production forest integration | HF is configured to help protect one production domain | This project focuses on safeguarding one identified Active Directory domain. Only this single domain with up to 20 DCs is in scope for this project.  Microsoft will configure HF with up to 4 DCs, located on up to 2 different network segments (subnets). | Additional domains and forests, if present, can be added as cost options to this project.  More than 20 production DCs can be supported by scaling HF components accordingly – as cost option on this project |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Integration with other DCs will be done by the customer. |  |
| Operations | Assist with defining roles and administrative functions for  HF ownership | Define practices and procedures. | or a service partner will run and maintain  the HF infrastructure. |
| Operational guidance | Document the recommended operational guidance and practices for using and maintaining the security infrastructure and  systems within the HF | Document will include practices and procedures to reflect service ownership functions and roles. |  |
| One deployment | HF is deployed once in the secure room and tested against a simulated production Active Directory Domain Services (AD DS). The same HF implementation is then used in the production. | HF is deployed once in the secure room and first connected to the simulated production Active Directory environment. After testing is complete, the HF is disconnected from the simulated Active Directory environment, moved to the datacenter, and connected to the production Active  Directory environment. | Additional deployments (dedicated lab deployment and new production deployment) are available as add-ons at cost. |
| Lab deployment | Dedicated lab deployment and additional production deployment | With this option HF is first deployed in a lab where it is tested against a lab or simulated production Active Directory Domain Services environment. After the HF is tested, a second HF is deployed for the production environment, and the lab  deployment stays. |  |
| Concept for Remote access integration | Conceptional work remote access support for HF workstations in production forest (based on a Threat Model) | This conceptional design will integrate technologies’ current remote access software onto the solution’s administrative desktop image. | For security reasons, remote access to HF workstations is not allowed.  Remote access software must:   * Be compatible with the selected admin workstation operating system (Windows 10 Enterprise x64). * Be able to operate concurrently with the   native operating system |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | IPsec capability, thereby not disabling it during installation or operation |
| Hardware security module (HSM) | Use HSM for CA operations | Deploy new or integrate with existing HSM in environments. | HSM must be compatible with Active Directory Certification Services.  Customer needs to provide a compatible HSM to be  integrated. |

The following optional components are out-of-scope and therefore not included in the general project scope:

Table 2: Optional Components and Features

|  |  |  |  |
| --- | --- | --- | --- |
| Optional Solution Component | Optional In-Scope Feature | Description and Considerations | Scope Assumptions |
| Subordinate CA | Integrate HF CA with existing infrastructure | Deploy HF CA as a subordinate CA, and then integrate with certificate revocation list publishing configuration or Online Certificate Status  Protocol configuration. |  |
| Security information and event management (SIEM) | Integration with existing SIEM | Establish a data connection and define filters so that events from HF monitoring can be collected in central SIEM  solution. |  |
| Additional domains or forests | Integration of more than one production Active Directory domain | The standard scope covers one production domain. More domains or forests can be integrated. |  |
| Backup | Integration with existing backup solution | Deploy backup agents, test HF configuration, and assess security posture with this  additional component. |  |
| Hyper-V high availability | High availability for the Hyper-V platform | Hyper-V clusters or Hyper-V, live migration and Hyper-V replica solutions. |  |
| Larger Active Directory environment | Designing HF components to manage larger Active Directory environment  (more than 20 DCs) | The base HF design scales to 20 domain controllers. If the production environment has  more than 20 DCs, the HF base |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | solution components must be scaled accordingly.  This might include:   * Larger virtual machine sizes for servers * More disk space for virtual machines * Dedicated SQL Server for SCOM * Scaled-out SCOM design   and implementation |  |

### Software Products and Technologies

The following software and licenses are required for implementation. It is ’ responsibility to procure the software and licenses described.

**Important Note:** Unless otherwise agreed in writing in the Work Order, temporarily appoints Microsoft to act as its agent for the limited purpose of evaluation and agreeing to the end-user terms of any click through license agreement that accompanies the software (Microsoft or non-Microsoft) listed in this SOW or the Work Order and included within the test and development environments. Customer can read these terms at any time by clicking the **About** box in the toolbar ribbon for the specific product, at [www.microsoft.com,](http://www.microsoft.com/) or by requesting a copy from the Microsoft Engagement Manager.

Unless otherwise agreed in writing in the Work Order, temporarily entitles Microsoft to act as its agent for the download of all required software. Acting on this entitlement, Microsoft can apply the Known Good Media Process to download and validate all required software, and can compile the software into a specific disk image structure that can be used directly to build the MDT server.

Table 3: Software Products (Paid Licenses)

|  |  |
| --- | --- |
| Operating Systems and Server Applications  (Paid Licenses) | Provided By |
| Windows Server 20 2016 or higher |  |
| Windows 10 Enterprise x64 |  |
| Microsoft SQL Server Standard 2014 or higher |  |
| System Center Operations Manager 2012 R2 x64 or  higher |  |
| System Center Configuration Manager 2012 R2 x64  or higher |  |

The following software packages will be required by the solution and are available as Internet downloads at no cost. Microsoft will provide a text file with all packages, versions, and their respective download locations. A script will be provided to download all required files.

Table 4: Software Products (Downloads)

|  |  |
| --- | --- |
| Name | Provided By |
| Microsoft BGInfo (from Sysinternals Suite) |  |
| Microsoft Assessment and Deployment Kit |  |
| Windows Management Framework |  |
| Microsoft Report Viewer |  |
| Microsoft Deployment Toolkit |  |
| Microsoft .NET Framework |  |
| Microsoft Attack Service Analyzer |  |
| Microsoft Enhanced Mitigation Experience Toolkit |  |
| Microsoft Network Monitor |  |
| Microsoft Message Analyzer |  |
| Microsoft SQL Server Data-Tier Application Framework |  |
| Microsoft SQL Server Feature Pack |  |
| Remote Server Administration Tools for Windows |  |
| Microsoft LAPS |  |
| Microsoft TCPView (from Sysinternals Suite) |  |
| Microsoft Process Explorer (from Sysinternals Suite) |  |
| Microsoft Process Monitor (from Sysinternals Suite) |  |
| Microsoft PsTools (from Sysinternals Suite) |  |
| Microsoft Security Compliance Manager |  |
| Administrative Templates for Windows |  |
| System Center Operations Manager Management Packs |  |

### Data Migration

Any data migration is out of scope for this project.

### Integration and Interfaces

The HF environment has interfaces with the following productive system in environment.

Table 5: Interface Scope

|  |  |  |  |
| --- | --- | --- | --- |
| Interface Name | Description | In Scope | Responsibility |
| AD1 | Active Directory trust relationship | An outgoing forest trust will be established from the production domain to the HF forest. |  |

### Environments

The following system environments describe the development and test facilities to be used by the project team members. For the following environments, will be responsible for the allocation and setup of the base hardware, network hardware, and network connectivity, and will provide all required software. The joint Microsoft and team will install and configure the software products in Table 3 and Table 4 as described in Section 1.2.1 of this document.

Table 6: Required Environments

|  |  |  |  |
| --- | --- | --- | --- |
| Environment | Location | Responsibility | Ready By |
| Build | Dedicated secure room |  | Before the Build phase of this project |
| Production | Secure datacenter |  | Before the Deploy phase of this project |

### Training and Knowledge Transfer

Informal knowledge transfer will be provided throughout the project. Informal knowledge transfer is defined as informal activities that occur when staff works side by side with Microsoft, and include whiteboard discussions, email threads, conference calls, and facilitated meetings on technical topics. Transfer activities are secondary to completing outcome and maintaining the project schedule. No outcome or meeting summary will be provided for these sessions or activities.

## 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:

Table 7: Areas Out of Scope

|  |  |
| --- | --- |
| Out of Scope—Component or Feature | Description and Considerations |
| Physical server setup, management, and maintenance | Physical server setup, installation, and networking  interfaces or evaluation of new hardware and software. Ongoing production operational support. |
| Remote access and administration of Tier 0 | This project does not recommend the use of remote administration for Tier 0 services, essentially the DCs. Direct network access to the HF forest is recommended, although remote options can be included as cost options. |
| Multiple domain or forest support | This project focuses only on the core production domain. It will not provide a model for the management of other domains or forests. However, the customer can use the administration environment built by this project to  administer other forests in the future. |
| Support for integrating more than 20 DCs | Base HF design supports up to 20 production DCs. Support for more DCs is optional and comes at additional cost. |

|  |  |
| --- | --- |
| Hardware | Hardware will not be provided under this Work Order. is responsible for acquiring all necessary hardware required as a result of this Work  Order. |
| Disaster recovery | Setup and configuration of disaster recovery sites at multiple datacenters. Fault tolerance and clustering for high availability or disaster recovery is out of scope. |
| Server and client licenses | Procurement of required server licenses or client access  licenses, including external connectors. |
| Networking services | Setup or configuration of network load-balancing servers or services, including security-enhanced reverse-proxy publishing mechanisms. |
| Operations | Operational assessments, improvement plans, or designs for new operational processes and procedures beyond the documented guidance as cooperated within the  operations guide document. |
| Current production environment | Changes to the current environment to resolve issues not related to the defined scope of this project. |
| Third-party software support | Microsoft will not be responsible for integration or  support of ’ third-party software. |
| Monitoring services | Setup or configuration of monitoring, auditing, and alerting services to actively monitor the health of the environment beyond any items explicitly included in  scope. |
| Migration or consolidation | Migration, consolidation, or rationalization of Active Directory objects such as users, groups, workstations, servers, applications, and group policies (including logon scripts), or any data migration. |
| Formal training | Formal classroom or hands-on lab training. |
| Test environment | Microsoft will not build a test environment. Microsoft will not duplicate ’ existing Windows corporate domain environment within a test lab or create Technologies’ test domains to simulate the production  domains. Microsoft will not run test cases. |
| Support | Post-deployment support. Additional support can be purchased separately. |
| Systems runbooks and playbooks | Preparation of systems runbooks and playbooks. |
| Older operating systems | Support for admin desktops that use an operating system version or image configuration other than those included in the project scope. |
| Improving the security on any services other than DCs and associated forest or domain-level administration accounts | This project looks only at securing Tier 0 of the Active Directory infrastructure. Providing a secure administration environment for standard user workstations or laptops and for applications servers (such as Exchange,  SharePoint, or SQL Server) is out of scope. |
| General production domain hardening | HF helps secure only Tier 0 user accounts; it does not  secure other components of Active Directory Domain |

|  |  |
| --- | --- |
|  | Services. General hardening of servers such as DCs is out of scope. |

# Project Approach and Timeline

This chapter details the project approach and timeline.

## Approach

Microsoft Services will make use of the Microsoft Solutions Framework (MSF) to implement this project. The project will be managed through structured phases by using phase-gate milestones and outcome to mark the approved completion of each phase before moving to the next phase. This project will include the following phases:

* Envision
* Plan
* Build
* Stabilize
* Deploy

The subsequent sections outline project activities and service outcome. Service outcome that require formal sign-off from to transition to the next phase of the project are noted as such.

### Envision Phase

During the Envision phase, Microsoft and will work together to establish the project technical requirements, goals, critical success factors, constraints, and details of the current environment.

The team will kick off the project with a series of envisioning working sessions with the key stakeholders to verify requirements and gather data on the existing environment. Microsoft will then create a project vision and scope document that will serve as the project’s charter, align expectations among the project team and stakeholders, and document all requirements.

The Envision phase ends when the vision and scope document is approved by . This milestone represents that the team agrees on the vision, the project direction, and the specific scope of work necessary to bring the vision to reality.

Microsoft will support the customer in the following areas marked as “Key Microsoft activities”:

##### Envision: Entrance Criteria

Table 8: Envision Phase Entrance Criteria

|  |  |
| --- | --- |
|  | Envision Phase Entrance Criteria |
| Business goals and objectives are documented | |

##### Envision: Key Microsoft Activities

Table 9: Envision Phase Key Microsoft Activities

|  |  |  |
| --- | --- | --- |
| **Activity** | **Covering** | **Description** |
| Workshop | Project kick-off covering team members, objectives, and outcome framework | Includes current state, requirements, and end-state objectives |
| Design sessions | Conceptual architecture discussions with the architects and  stakeholders | Microsoft and team will review the solution elements and features for each solution component in Table 1: Services in Scope |
| Document | Record the conceptual design in the vision and scope document | Envisioning phase milestone outcome that describes the objectives, approach, and conceptual design for the project |
| Review | Review the vision and scope document | Microsoft and team will review  the document and prepare for sign-off |
| Document | Project plan with key milestones | Draft high-level project plan with key milestones |

##### Envision: Key Customer Activities

Table 10: Envision Phase Key Activities

|  |
| --- |
| **Activity** |
| Provide any necessary communication or information in preparation for requests that might result from discussions during the Envision workshop, including information-gathering exercises |
| Participate in the review and approval process of the vision and scope document outcome |
| Work with Microsoft to identify the project team members |
| Make decisions when architectural options are presented |
| Engage operations and service owners in raising awareness of the new systems to be implemented |
| Process change management approvals as required |
| Develop communication plan |

##### Envision: Documentations

**Table 11: Envision Phase Documentations**

|  |
| --- |
| **Documentations** |
| Vision and scope document |
| Draft project plan and milestone planning |

**Envision: Key Work Products and Outcome ()**

Table 12: Envision Phase Key Work Products and Outcome ()

|  |
| --- |
| **Key Work Products and Outcome ()** |
| Information as requested |
| Decisions |
| Change management approvals |

|  |
| --- |
| Communication plan |

##### Envision: Key Phase Assumptions

Table 13: Envision Phase Key Assumptions

|  |
| --- |
| **Key Phase Assumptions** |
| service owners and architects are identified and can attend and participate in the HF envisioning workshop |
| Current configuration and data descriptions are available |
| Functional requirements are documented |

##### Envision: Exit Criteria

Table 14: Envision Phase Exit Criteria

|  |
| --- |
| Envision Phase Exit Criteria |
| Vision and scope document is evaluated |
| Draft project plan and milestone planning are prepared |

### Plan Phase

During the Plan phase, Microsoft will work with to develop and meet the technical and functional requirements in the logical and physical designs, and to define and describe the environment end state. Microsoft will record the HF design in the architecture and design document. The project plan will be updated to reflect the detailed timeline for the Build, Stabilize, and Deploy phases.

The Plan phase will be considered complete upon the ’ evaluation of the architecture and design document.

Microsoft will support the customer in the following areas marked as “Key Microsoft activities”:

##### Plan: Entrance Criteria

Table 15: Plan Phase Entrance Criteria

|  |
| --- |
| Plan Phase Entrance Criteria |
| Vision and scope document is evaluated from Envision phase |
| Draft project plan and milestone planning are prepared from Envision phase |

##### Plan: Key Microsoft Activities

Table 16: Plan Phase Key Microsoft Activities

|  |  |  |
| --- | --- | --- |
| **Activity** | **Covering** | **Description** |
| Design sessions | HF solution components | Activity: establish functional definitions for each component of this element defined in Table 1:  Services in Scope |
| Document | Record the design within the architecture and design document | Outcome: describes the solution and its components, logical solution, and physical implementation. |

|  |  |  |
| --- | --- | --- |
| Review | Review the architecture and design document | * Activity: confirm functional design and description as outlined in this document. * sign-off is required. |
| Review | Review project plan | * Review and update the project plan to reflect customer-specific dependencies and logistical constraints for the Build, Stabilize, and Deploy phases. * Work product does not require sign-off. |

##### Plan: Key Customer Activities

Table 17: Plan Phase Key Activities

|  |
| --- |
| **Activity** |
| Facilitate any necessary communication or information in preparation for requests that might result from discussions during the Planning design sessions, including information-gathering exercises. |
| Participate in the review and approval process of the architecture and design document outcome. |
| subject matter experts (SMEs) are engaged to participate in the design sessions and are making decisions when architectural options are presented. |

##### Plan: Documentations

Table 18: Plan Phase Documentations

Architecture and design document

**Documentations**

##### Plan: Key Work Products and Outcome ()

Table 19: Plan Phase Key Work Products and Outcome ()

|  |
| --- |
| **Key Work Products and Outcome ()** |
| Information as requested |
| Decisions |
| Change management approvals |

##### Plan: Key Phase Assumptions

Table 20: Plan Phase Key Assumptions

|  |
| --- |
| Key Phase Assumptions |
| None |

##### Plan: Exit Criteria

Table 21: Plan Phase Exit Criteria

|  |
| --- |
| Plan Phase Exit Criteria |
| Architecture and design document is evaluated. |

### Build Phase

During the Build phase, the team builds the HF solution components within the secure room. The goal of this phase is to help the team to connect the HF deployment to the simulated production Active Directory environment.

Microsoft will support the customer in the following areas marked as “Key Microsoft activities”:

##### Build: Entrance Criteria

Table 22: Build Phase Entrance Criteria

|  |
| --- |
| **Key Phase Entrance Criteria** |
| Architecture and design document are evaluated. |

##### Build: Key Microsoft Activities

Table 23: Build Phase Key Microsoft Activities

|  |  |  |
| --- | --- | --- |
| **Activity** | **Covering** | **Description** |
| Build sessions | HF solution | * Implement HF solution in secure room. * Establish build definitions for each HF solution component as defined in Table 1: Services in   Scope. |
| Document | Test guide document | Work product: describes the testing of HF functionality, not to include - specific test cases. |
| Review | Review test guide | Work product: does not require  sign-off. |
| Document | Update the build process within the implementation guide document | This document contains the configuration information necessary to build the end-state system as described in the architecture and design document. |
| Review | Review the implementation guide document with Vitesco  technologies. | Confirm build definitions as represented in the architecture and design document; sign-off is required. |

##### Build: Key Customer Activities

Table 24: Build Phase Key Activities

|  |
| --- |
| **Activity** |
| Participate in Build activities |

##### Build: Documentations

Table 25: Build Phase Documentations

Documentations

|  |
| --- |
| HF deployed and connected to simulated production Active Directory |
| Implementation guide document |
| Test guide |

##### Build: Key Work Products and Outcome ()

Table 26: Plan Phase Key Work Products and Outcome ()

|  |
| --- |
| **Key Work Products and Outcome ()** |
| Information as requested |
| Decisions |
| Change management approvals |

##### Build: Key Phase Assumptions

Table 27: Build Phase Key Assumptions

|  |
| --- |
| Key Phase Assumptions |
| SMEs are engaged to participate in the development sessions. |
| will provide appropriate secure room facilities, including hardware and software, to simulate production. |

##### Build: Exit Criteria

Table 28: Build Phase Exit Criteria

|  |
| --- |
| Key Phase Exit Criteria |
| HF deployed and connected to simulated production Active Directory environment. |
| Implementation guide is completed. |
| Test guide is completed. |

### Stabilize Phase

During the Stabilize phase, the combined Microsoft and team will implement the test guide in the secure room, document the results for all test cases, and validate the build process.

Microsoft will record the recommended operational practices and procedures in the operations guide.

The Stabilize phase ends with the solution having been verified through the implementation of the test guide by and with the completion and evaluation of all outcome that require formal evaluation.

Microsoft will support the customer in the following areas marked as “Key Microsoft activities”:

##### Stabilize: Entrance Criteria

Table 29: Stabilize Phase Entrance Criteria

|  |
| --- |
| Key Phase Entrance Criteria |
| HF deployed and connected to simulated production Active Directory environment. |

##### Stabilize: Key Microsoft Activities

Table 30: Stabilize Phase Key Microsoft Activities

|  |  |  |
| --- | --- | --- |
| **Activity** | **Covering** | **Description** |
| Functional testing | * Run test cases from test guide * Document test results | The approximate durations of the activities are as follows:   * On-board test users: 1 day * Run Microsoft HF test guide: 2 days * Run customer-specific test guide: 5 days * Update test guide (if needed): 1 day |
| Document | Update the operational procedures in the operations guide document | The document includes specific operational guidance for the systems and components described in the architecture and design document |
| Review | Review the operations  guide with | Confirm operational practices and procedures as  documented in this outcome; sign-off is required |

##### Stabilize: Key Customer Activities

Table 31: Stabilize Phase Key Activities

|  |
| --- |
| **Activity** |
| Engage designated test users |
| Perform system testing based on the test guide |
| Participate in the review and approval process of the implementation guide document |
| Participate in the review and approval process of the operations guide document |

##### Stabilize: Documentations

Table 32: Stabilize Phase Documentations

|  |
| --- |
| Documentations |
| HF test cases complete |
| Operations guide document |

##### Stabilize: Key Work Products and Outcome ()

Table 33: Plan Phase Key Work Products and Outcome ()

|  |
| --- |
| **Key Work Products and Outcome ()** |
| Information as requested |
| Decisions |
| Change management approvals |
| Test result documentation (test results in test guide tables) |

##### Stabilize: Key Phase Assumptions

Table 34: Stabilize Phase Key Assumptions

SMEs and test users are engaged to participate in the testing activities.

**Key Phase Assumptions**

Post-deployment support process will be established by prior to commencement of the Deploy phase.

will provide appropriate lab facilities, including hardware and software, to conduct testing.

##### Stabilize: Exit Criteria

Table 35: Stabilize Phase Exit Criteria

|  |
| --- |
| **Key Phase Exit Criteria** |
| Functional testing is completed. P1 and P2 defects fixed. |
| Implementation guide is approved. |
| Operations guide is approved. |

### Deploy Phase

The Deploy phase begins with the implementation of the HF solution for production use. The HF deployment in the secure room is disconnected from the simulated production Active Directory environment, and the servers are moved to the datacenter and connected to the real production Active Directory environment.

The ’ users will validate the solution functionality in the production environment based on the operations guide. will have three days to validate the functionality of the new administrative environment within their organization.

After the validation tests are completed, the production rollout begins with ’ administrators using the solution to perform their daily work. During the rollout, these administrators report any issues that need to be addressed and work with Microsoft to troubleshoot and resolve these issues.

Microsoft will support the customer in the following areas marked as “Key Microsoft activities”:

##### Deploy: Entrance Criteria

Table 36: Deploy Phase Entrance Criteria

|  |
| --- |
| **Key Phase Entrance Criteria** |
| Implementation guide approved. |
| Operations guide approved. |
| All -furnished, pre-deployment information will be provided no later than seven days prior to the start of Deploy phase. |
| Administrative processes will be established by prior to commencement of the  Deploy phase. |

##### Deploy: Key Microsoft Activities

Table 37: Deploy Phase Key Microsoft Activities

|  |  |  |
| --- | --- | --- |
| **Activity** | **Covering** | **Description** |
| Deploy sessions | Connect HF to the production environment | * HF production implementation: Microsoft will assist as needed while puts the implementation guide into effect. * Microsoft support activities are limited to the first 20 DCs in production forest. |
| Handover and  closeout | Handover and closeout of  project | General assistance to  staff for handover and closeout. |

##### Deploy: Key Customer Activities

Table 38: Deploy Phase Key Activities

|  |
| --- |
| **Activity** |
| Deploy solution to production |
| Provide direction to the Microsoft resources during this project phase |
| Run customer evaluation tests |
| Provide feedback on production use |

##### Deploy: Documentations

Table 39: Deploy Phase Documentations

Support for HF production implementation

**Documentations**

##### Deploy: Key Work Products and Outcome ()

Table 40: Plan Phase Key Work Products and Outcome ()

|  |
| --- |
| **Key Work Products and Outcome ()** |
| Information as requested |
| Decisions |
| Change management approvals |
| Written feedback on production functionality |

##### Deploy: Key Phase Assumptions

Table 41: Deploy Phase Key Assumptions

|  |
| --- |
| Key Phase Assumptions |
| will own their change control process. |
| Affected organizations will identify named resources and groups that will be required for the Deploy phase. |

|  |
| --- |
| In performing our services under this SOW and the applicable Work Order for this project phase, we will rely upon any instructions, authorizations, approvals, or other information provided to us by ’ Project Manager or by any other personnel identified by your Project Manager. |
| The deployment process for one production domain and 20 DCs will help the customer to continue  and finalize HF integration of all production DCs. |

##### Deploy: Exit Criteria

Table 42: Deploy Phase Exit Criteria

|  |  |
| --- | --- |
|  | Key Phase Exit Criteria |
| HF production implementation is complete | |
| Customer evaluation test successfully completed | |

## Timeline

It is estimated that this engagement will be performed in approximately three months and will include the phases and milestones noted. The actual timeline for this engagement will be relative to the project start date, and all dates and durations provided are estimates only.

Customer Project Manager

Microsoft Project Manager

Customer Project Sponsor

# Project Organization and Staffing

## Project Organization Structure

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

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



Executive Steering Committee

Microsoft Engagement Manager

Microsoft Lead Architect

Partner Team Leader

Customer Role 2

Customer Role 1

Partner Role 1

Microsoft Role 1

Figure 1: Project organization structure

## Project Roles and Responsibilities

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

#### Customer Project Roles and Responsibilities

Table 43: Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Project Sponsor | Makes key project decisions, assists in escalating unresolved issues to the executive steering committee, and clears  project roadblocks | Part-time availability with expected allocation of 2–4 hours per week |
| 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 cooperate outcome according to the project schedule | Full-time availability with expected allocation of 20–40 hours |
| Technical Team Lead | Primary technical point of contact for the team that is responsible for technical architecture and code outcome | Full-time availability with expected allocation of 16–40 hours per week |
| Technical Architect | QA and escalation of technical decisions  and issues | Full-time availability with expected  allocation of 4–12 hours per week |
| Test and QA Lead | Test plans and guides, coordinating testing resources for evaluation tests | Full-time availability with expected allocation of 4–12 hours per week |
| Active Directory  SMEs | Technical representation for Active  Directory Domain Services | Full-time availability with expected  allocation of 4–12 hours per week |
| Security SMEs | Technical representation for cybersecurity that relates to the security architecture to  be implemented | Full-time availability with expected allocation of 4–12 hours per week |
| Other SMEs | Technical representation for related systems and services, including network, DNS, PKI, and smart card integration | Full-time availability with expected allocation of 4–12 hours per week |

#### Microsoft Project Roles and Responsibilities

Table 44: Microsoft Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Microsoft Architects | * Provide technical oversight | Part time |

|  |  |  |
| --- | --- | --- |
|  | * Verify whether Microsoft- recommended practices are followed * Responsible for overall technical   solution management |  |
| Microsoft Consultants | * Technical design leadership * Cooperate of all workshops and sessions * Development of technical outcome | Full time |