Cybersecurity Response Program

Statement of Work

Prepared for

**CUSTOMER NAME REMOVED**

Prepared by

**Microsoft Services**

Date: 5th Feb 2020

Version: 2.3

Table of contents

[Common Terms and Abbreviations 10](#_Toc20902292)

[Introduction 13](#_Toc20902293)

[1. Program objectives and scope 15](#_Toc20902294)

[1.1. Objectives 15](#_Toc20902295)

[1.2. Outcomes 16](#_Toc20902296)

[1.3. Areas in scope 16](#_Toc20902297)

[1.3.1. General program scope 16](#_Toc20902298)

[1.3.2. Software products and technologies 23](#_Toc20902299)

[1.4. Areas out of scope 23](#_Toc20902300)

[2. Program approach, timeline, and deliverables 25](#_Toc20902301)

[2.1. Approach 25](#_Toc20902302)

[2.1.1. Program dependencies 26](#_Toc20902303)

[2.1.2. Program initiation 26](#_Toc20902304)

[2.1.3. Program planning 29](#_Toc20902305)

[2.1.4. Program executing and controlling 29](#_Toc20902306)

[2.1.5. Program closing 30](#_Toc20902307)

[2.2. Program timeline 31](#_Toc20902308)

[2.3. Program Pre-Requisites / Dependencies 32](#_Toc20902309)

[2.4. Program deliverables 33](#_Toc20902310)

[2.5. Deliverable acceptance process 34](#_Toc20902311)

[2.6. Defect remediation 34](#_Toc20902312)

[2.7. Program governance 35](#_Toc20902313)

[2.7.1. Program communication 35](#_Toc20902314)

[2.7.2. Program risk and issue management 35](#_Toc20902315)

[2.7.3. Change management process 36](#_Toc20902316)

[2.7.4. Executive Steering Committee 37](#_Toc20902317)

[2.7.5. Escalation path 37](#_Toc20902318)

[2.7.6. Architectural Review Board 38](#_Toc20902319)

[2.8. Program completion 39](#_Toc20902320)

[3. Program organisation 40](#_Toc20902321)

[3.1. Program structure 40](#_Toc20902322)

[3.2. Program roles and responsibilities 40](#_Toc20902323)

[3.2.1. CUSTOMER NAME REMOVED 40](#_Toc20902324)

[3.2.2. Microsoft 43](#_Toc20902325)

[4. CUSTOMER NAME REMOVED responsibilities and program assumptions 46](#_Toc20902326)

[4.1. CUSTOMER NAME REMOVED responsibilities 46](#_Toc20902327)

[4.2. Program assumptions 46](#_Toc20902328)

[5. P01: Active Directory Hardening (ADH) 48](#_Toc20902329)

[5.1. Objectives 48](#_Toc20902330)

[5.2. Areas in scope 49](#_Toc20902331)

[5.2.1. General project scope 49](#_Toc20902332)

[5.2.2. Environments 51](#_Toc20902333)

[5.2.3. Testing 52](#_Toc20902334)

[5.2.4. Training 52](#_Toc20902335)

[5.3. Areas out of scope 53](#_Toc20902336)

[5.4. Approach 53](#_Toc20902337)

[5.4.1. Envision 54](#_Toc20902338)

[5.4.2. Plan 54](#_Toc20902339)

[5.4.3. Build 55](#_Toc20902340)

[5.4.4. Stabilise 56](#_Toc20902341)

[5.4.5. Deploy 56](#_Toc20902342)

[5.5. Deliverables 57](#_Toc20902343)

[5.6. Project roles and responsibilities 58](#_Toc20902344)

[5.6.1. CUSTOMER NAME REMOVED 58](#_Toc20902345)

[5.6.2. Microsoft 59](#_Toc20902346)

[5.7. CUSTOMER NAME REMOVED responsibilities and project assumptions 59](#_Toc20902347)

[5.7.1. CUSTOMER NAME REMOVED responsibilities 59](#_Toc20902348)

[5.7.2. Project assumptions 59](#_Toc20902349)

[6. P02: Enhanced Security Administrative Environment (ESAE) 60](#_Toc20902350)

[6.1. Objectives 60](#_Toc20902351)

[6.2. Areas in scope 60](#_Toc20902352)

[6.2.1. General project scope 60](#_Toc20902353)

[6.2.2. Software products and technologies 62](#_Toc20902354)

[6.2.3. Environments 63](#_Toc20902355)

[6.2.4. Testing 63](#_Toc20902356)

[6.3. Areas out of scope 64](#_Toc20902357)

[6.4. Approach 65](#_Toc20902358)

[6.4.1. Envision 65](#_Toc20902359)

[6.4.2. Plan 66](#_Toc20902360)

[6.4.3. Build 66](#_Toc20902361)

[6.4.4. Stabilise 67](#_Toc20902362)

[6.4.5. Deploy 68](#_Toc20902363)

[6.5. Deliverables 68](#_Toc20902364)

[6.6. Project roles and responsibilities 70](#_Toc20902365)

[6.6.1. CUSTOMER NAME REMOVED 70](#_Toc20902366)

[6.6.2. Microsoft 70](#_Toc20902367)

[7. P03: Privileged Access Workstation (PAW) – Tier 1 71](#_Toc20902368)

[7.1. Objectives 71](#_Toc20902369)

[7.2. Areas in scope 72](#_Toc20902370)

[7.2.1. General project scope 72](#_Toc20902371)

[7.2.2. Software products and technologies 75](#_Toc20902372)

[7.2.3. System integration 76](#_Toc20902373)

[7.2.4. Environments 76](#_Toc20902374)

[7.2.5. Testing 77](#_Toc20902375)

[7.3. Areas out of scope 77](#_Toc20902376)

[7.4. Approach 78](#_Toc20902377)

[7.4.1. Envision 79](#_Toc20902378)

[7.4.2. Plan 79](#_Toc20902379)

[7.4.3. Build 80](#_Toc20902380)

[7.4.4. Stabilise 81](#_Toc20902381)

[7.4.5. Deploy 82](#_Toc20902382)

[7.5. Deliverables 82](#_Toc20902383)

[7.6. Project roles and responsibilities 83](#_Toc20902384)

[7.6.1. CUSTOMER NAME REMOVED 83](#_Toc20902385)

[7.6.2. Microsoft 83](#_Toc20902386)

[7.7. CUSTOMER NAME REMOVED responsibilities 84](#_Toc20902387)

[7.8. Project assumption 84](#_Toc20902388)

[8. P04: Azure Security Foundations (ASF) 85](#_Toc20902389)

[8.1. Objectives 85](#_Toc20902390)

[8.2. Areas in scope 85](#_Toc20902391)

[8.2.1. General project scope 85](#_Toc20902392)

[8.3. Areas out of scope 87](#_Toc20902393)

[8.4. Testing 88](#_Toc20902394)

[8.5. Approach 88](#_Toc20902395)

[8.5.1. Assess 88](#_Toc20902396)

[8.5.2. Enable 90](#_Toc20902397)

[8.6. Deliverables 90](#_Toc20902398)

[8.7. Project roles and responsibilities 92](#_Toc20902399)

[8.7.1. CUSTOMER NAME REMOVED 92](#_Toc20902400)

[8.7.2. Microsoft 92](#_Toc20902401)

[9. P05: Azure Cloud Privileged Access Workstation (PAW) 93](#_Toc20902402)

[9.1. Objectives 93](#_Toc20902403)

[9.2. Areas in scope 94](#_Toc20902404)

[9.2.1. General project scope 94](#_Toc20902405)

[9.2.2. Software products and technologies 96](#_Toc20902406)

[9.2.3. System integration 97](#_Toc20902407)

[9.2.4. Environments 97](#_Toc20902408)

[9.2.5. Testing and defect remediation 98](#_Toc20902409)

[9.3. Areas out of scope 99](#_Toc20902410)

[9.4. Project approach 100](#_Toc20902411)

[9.4.1. Approach 100](#_Toc20902412)

[9.5. Deliverables 103](#_Toc20902413)

[9.6. Project roles and responsibilities 104](#_Toc20902414)

[9.6.1. CUSTOMER NAME REMOVED 104](#_Toc20902415)

[9.6.2. Microsoft 104](#_Toc20902416)

[9.6.3. CUSTOMER NAME REMOVED responsibilities 104](#_Toc20902417)

[10. P06: Advanced Threat Detection Implementation Services (ATDIS) 106](#_Toc20902418)

[10.1. Objectives 106](#_Toc20902419)

[10.2. Areas in scope 106](#_Toc20902420)

[10.2.1. General project scope 106](#_Toc20902421)

[10.2.2. Software products and technologies 108](#_Toc20902422)

[10.2.3. Environments 108](#_Toc20902423)

[10.2.4. Testing 109](#_Toc20902424)

[10.2.5. Workshops 109](#_Toc20902425)

[10.3. Areas out of scope 115](#_Toc20902426)

[10.4. Project approach 116](#_Toc20902427)

[10.4.1. Approach 116](#_Toc20902428)

[10.4.2. Assess 116](#_Toc20902429)

[10.4.3. Remediate 118](#_Toc20902430)

[10.4.4. Enable 119](#_Toc20902431)

[10.5. Deliverables 122](#_Toc20902432)

[10.6. Project roles and responsibilities 124](#_Toc20902433)

[10.6.1. CUSTOMER NAME REMOVED 124](#_Toc20902434)

[10.6.2. Microsoft 124](#_Toc20902435)

[11. P07: Modern Desktop Deployment (MDD) 125](#_Toc20902436)

[11.1. Objectives 125](#_Toc20902437)

[11.2. Areas in scope 125](#_Toc20902438)

[11.2.1. General project scope 125](#_Toc20902439)

[11.2.2. Software products and technologies 128](#_Toc20902440)

[11.2.3. Environments 128](#_Toc20902441)

[11.2.4. Testing 128](#_Toc20902442)

[11.3. Areas out of scope 129](#_Toc20902443)

[11.4. Approach 130](#_Toc20902444)

[11.4.1. Assess 131](#_Toc20902445)

[11.4.2. Remediate 132](#_Toc20902446)

[11.4.3. Enable 132](#_Toc20902447)

[11.5. Deliverables 135](#_Toc20902448)

[11.6. Project roles and responsibilities 137](#_Toc20902449)

[11.6.1. CUSTOMER NAME REMOVED 137](#_Toc20902450)

[11.6.2. Microsoft 137](#_Toc20902451)

[12. P08: Modern Server Deployment (MSD) 138](#_Toc20902452)

[12.1. Objectives 138](#_Toc20902453)

[12.2. Areas in scope 138](#_Toc20902454)

[12.2.1. General project scope 138](#_Toc20902455)

[12.2.2. Software products and technologies 140](#_Toc20902456)

[12.2.3. Environments 141](#_Toc20902457)

[12.2.4. Testing 141](#_Toc20902458)

[12.3. Areas out of scope 141](#_Toc20902459)

[12.4. Approach 143](#_Toc20902460)

[12.4.1. Assess 143](#_Toc20902461)

[12.4.2. Remediate 145](#_Toc20902462)

[12.4.3. Enable 145](#_Toc20902463)

[12.5. Deliverables 147](#_Toc20902464)

[12.6. Project roles and responsibilities 149](#_Toc20902465)

[12.6.1. CUSTOMER NAME REMOVED 149](#_Toc20902466)

[12.6.2. Microsoft 149](#_Toc20902467)

[13. P09: Operational Service Management (OSM) 150](#_Toc20902468)

[13.1. Objectives 150](#_Toc20902469)

[13.2. Areas in Scope 152](#_Toc20902470)

[13.2.1. General Project Scope 152](#_Toc20902471)

[13.3. Areas Out of Scope 156](#_Toc20902472)

[13.4. Project Approach 156](#_Toc20902473)

[13.4.1. Envision 156](#_Toc20902474)

[13.4.2. Plan 157](#_Toc20902475)

[13.4.3. Build 160](#_Toc20902476)

[13.4.4. Stabilise 160](#_Toc20902477)

[13.5. Deliverables 161](#_Toc20902478)

[13.6. Project Roles and Responsibilities 164](#_Toc20902479)

[13.6.1. CUSTOMER NAME REMOVED 164](#_Toc20902480)

[13.6.2. Microsoft 164](#_Toc20902481)

[14. P10: Adoption and Change Management (ACM) Assistance 165](#_Toc20902482)

[14.1. Objectives 165](#_Toc20902483)

[14.2. Areas in Scope 165](#_Toc20902484)

[14.2.1. General project scope 165](#_Toc20902485)

[14.2.2. Areas out of scope 165](#_Toc20902486)

[14.3. Project Approach 166](#_Toc20902487)

[14.3.1. Kick-off 166](#_Toc20902488)

[14.3.2. Progress review 167](#_Toc20902489)

[14.3.3. Close out 167](#_Toc20902490)

[14.4. Deliverables 167](#_Toc20902491)

[14.5. Project Roles and Responsibilities 168](#_Toc20902492)

[14.5.1. CUSTOMER NAME REMOVED 168](#_Toc20902493)

[14.5.2. Microsoft 168](#_Toc20902494)

[14.6. Project assumptions and preconditions 169](#_Toc20902495)

[14.6.1. Preconditions 169](#_Toc20902496)

[15. Conclusion 170](#_Toc20902497)

List of Tables

[Table 1: Common Terms and Abbreviations 10](#_Toc10544461)

[Table 2: General program scope 16](#_Toc10544462)

[Table 3: General program out of scope 23](#_Toc10544463)

[Table 4: Program dependencies 26](#_Toc10544464)

[Table 5: Program initiation activities 27](#_Toc10544465)

[Table 6: Program planning activities 29](#_Toc10544466)

[Table 7: Program executing and controlling activities 29](#_Toc10544467)

[Table 8: Program closing activities 30](#_Toc10544468)

[Table 9: Program Pre-Requisites/Dependencies 32](#_Toc10544469)

[Table 10: Defect Priorities 34](#_Toc10544470)

[Table 11: Program roles and responsibilities - CUSTOMER NAME REMOVED 41](#_Toc10544471)

[Table 12: Program roles and responsibilities - Microsoft 43](#_Toc10544472)

[Table 13: ADH – General project scope 49](#_Toc10544473)

[Table 14: ADH – Environments 51](#_Toc10544474)

[Table 15: ADH – Testing 51](#_Toc10544475)

[Table 16: ADH – Training 52](#_Toc10544476)

[Table 17: ADH – Out of scope 53](#_Toc10544477)

[Table 18: ADH – Envision activities 54](#_Toc10544478)

[Table 19: ADH – Plan activities 54](#_Toc10544479)

[Table 20: ADH – Build activities 55](#_Toc10544480)

[Table 21: ADH – Stabilise activities 56](#_Toc10544481)

[Table 22: ADH – Deploy activities 56](#_Toc10544482)

[Table 23: ADH – Deliverables 57](#_Toc10544483)

[Table 24: ADH – Microsoft roles and responsibilities 58](#_Toc10544484)

[Table 25: ESAE - General project scope 59](#_Toc10544485)

[Table 26: ESAE - Software products and technologies 61](#_Toc10544486)

[Table 27: ESAE - System environments 62](#_Toc10544487)

[Table 28: ESAE - Testing 63](#_Toc10544488)

[Table 29: ESAE - Out of scope 63](#_Toc10544489)

[Table 30 - ESAE - Envision phase 64](#_Toc10544490)

[Table 31: ESAE - Plan phase 65](#_Toc10544491)

[Table 32: ESAE - Build phase 65](#_Toc10544492)

[Table 33: ESAE - Stabilise phase 66](#_Toc10544493)

[Table 34: ESAE - Deploy Phase 67](#_Toc10544494)

[Table 35: ESAE – Deliverables 68](#_Toc10544495)

[Table 36: ESAE - Project roles and responsibilities - Microsoft 69](#_Toc10544496)

[Table 37: PAW T1 – General project scope 71](#_Toc10544497)

[Table 38: PAW T1 – Software products and technologies 74](#_Toc10544498)

[Table 39: PAW T1 – Other software products and technologies 74](#_Toc10544499)

[Table 40: PAW T1 – System integration 75](#_Toc10544500)

[Table 41: PAW T1 – Environments 75](#_Toc10544501)

[Table 42: PAW T1 – Testing 76](#_Toc10544502)

[Table 43: PAW T1 – Out of scope 76](#_Toc10544503)

[Table 44: PAW T1 – Envision activities 78](#_Toc10544504)

[Table 45: PAW T1 – Plan activities 78](#_Toc10544505)

[Table 46: PAW T1 – Build activities 79](#_Toc10544506)

[Table 47: PAW T1 – Stabilise activities 80](#_Toc10544507)

[Table 48: PAW T1 – Deploy activities 81](#_Toc10544508)

[Table 49: PAW T1 – Deliverables 81](#_Toc10544509)

[Table 50: PAW T1 – Microsoft roles and responsibilities 82](#_Toc10544510)

[Table 51: ASF - General project scope 84](#_Toc10544511)

[Table 52: ASF – Out of scope 86](#_Toc10544512)

[Table 53 ASF - Testing 87](#_Toc10544513)

[Table 54: ASF - Assess phase activities 88](#_Toc10544514)

[Table 55: ASF - Enable phase activities 89](#_Toc10544515)

[Table 56: ASF – Deliverables 89](#_Toc10544516)

[Table 57: ASF - Microsoft roles and responsibilities 91](#_Toc10544517)

[Table 58: PAW – General project scope 93](#_Toc10544518)

[Table 59: PAW - Software products and technologies 95](#_Toc10544519)

[Table 60: PAW - Software packages required 95](#_Toc10544520)

[Table 61: PAW - System integration in scope 96](#_Toc10544521)

[Table 62: PAW - Environments 96](#_Toc10544522)

[Table 63: PAW - Testing 97](#_Toc10544523)

[Table 64: PAW - Out of scope 98](#_Toc10544524)

[Table 65: PAW - Assess phase 99](#_Toc10544525)

[Table 66: PAW - Remediate phase 100](#_Toc10544526)

[Table 67: PAW - Enable phase 101](#_Toc10544527)

[Table 68: PAW – Deliverables 102](#_Toc10544528)

[Table 69: PAW - Microsoft roles and responsibilities 103](#_Toc10544529)

[Table 70: ATDIS – General project scope 106](#_Toc10544530)

[Table 71: ATDIS - Software products & technologies 107](#_Toc10544531)

[Table 72: ATDIS - Environments 107](#_Toc10544532)

[Table 73: ATDIS - Testing 108](#_Toc10544533)

[Table 74: ATDIS - Workshops 108](#_Toc10544534)

[Table 75: ATDIS - Out of scope 114](#_Toc10544535)

[Table 76: ATDIS - Assess phase 115](#_Toc10544536)

[Table 77: ATDIS - Remediate phase 117](#_Toc10544537)

[Table 78: ATDIS - Enable phase 118](#_Toc10544538)

[Table 79: ATDIS – Deliverables 121](#_Toc10544539)

[Table 80: ATDIS - Microsoft roles and responsibilities 123](#_Toc10544540)

[Table 81: MDD – General project scope 124](#_Toc10544541)

[Table 82: MDD - Software products and technologies 127](#_Toc10544542)

[Table 83: MDD - Environments required 127](#_Toc10544543)

[Table 84: MDD - Testing 127](#_Toc10544544)

[Table 85: MDD - Out of scope 128](#_Toc10544545)

[Table 86: MDD - Assess phase 130](#_Toc10544546)

[Table 87: MDD - Enable phase 131](#_Toc10544547)

[Table 88: MDD – Deliverables 134](#_Toc10544548)

[Table 89: MDD - Microsoft roles and responsibilities 136](#_Toc10544549)

[Table 90: General project scope 137](#_Toc10544550)

[Table 91: MSD - Software products and technologies 139](#_Toc10544551)

[Table 92: MSD - Environments 140](#_Toc10544552)

[Table 93: MSD - Testing 140](#_Toc10544553)

[Table 94: MSD - Out of scope 140](#_Toc10544554)

[Table 95: MSD - Assess phase 142](#_Toc10544555)

[Table 96: MSD - Enable phase 144](#_Toc10544556)

[Table 97: MSD – Deliverables 146](#_Toc10544557)

[Table 98: MSD - Microsoft Project roles and responsibilities 148](#_Toc10544558)

[Table 99: OSM - Overall project objectives 150](#_Toc10544559)

[Table 100: OSM – General project in scope 151](#_Toc10544560)

[Table 101: OSM - Out of scope 155](#_Toc10544561)

[Table 102: OSM - Envision Phase 155](#_Toc10544562)

[Table 103: OSM - Plan phase 156](#_Toc10544563)

[Table 104: OSM - Build phase 159](#_Toc10544564)

[Table 105: OSM - Stabilise phase 159](#_Toc10544565)

[Table 106: OSM – Deliverables 160](#_Toc10544566)

[Table 107: ACM - Out of scope 164](#_Toc10544567)

[Table 108: ACM – Kick-off phase 165](#_Toc10544568)

[Table 109: ACM – Progress review phase 166](#_Toc10544569)

[Table 110: ACM – Close out phase 166](#_Toc10544570)

[Table 111: ACM – Deliverables 167](#_Toc10544571)

List of Figures

[Figure 1 - Microsoft Cybersecurity Response Program 15](#_Toc10305353)

[Figure 2: Program Timeline 31](#_Toc10305354)

[Figure 3: Executive Steering Committee (ESC) 36](#_Toc10305355)

[Figure 4: Escalation Path 37](#_Toc10305356)

[Figure 5: Architectural Review Board 37](#_Toc10305357)

[Figure 6: Microsoft & CUSTOMER NAME REMOVED Program Organisation 39](#_Toc10305358)

[Figure 7: ADH – Approach 53](#_Toc10305359)

[Figure 8: ESAE - Approach 64](#_Toc10305360)

[Figure 9: PSW T1 – Approach 77](https://microsoft-my.sharepoint.com/personal/miholt_microsoft_com/Documents/My%20Work/Customers/CBA/0.FY19/DPG%20Lime%20Leopard/SOW/Cybersecurity%20Response%20Program%20SOW%20v1.0%20MH%20edit%20and%20Conclusion.docx#_Toc10305361)

[Figure 10: Azure Cloud PAW - Approach 99](#_Toc10305362)

[Figure 11: ATDIS - Approach 115](#_Toc10305363)

[Figure 12: MDD - Approach 129](#_Toc10305364)

[Figure 13: MSD - Approach 142](#_Toc10305365)

This Statement of Work (SOW) and any exhibits, appendices, schedules, and attachments to it are made pursuant to Work Order 7-SP4WUARY4 and describes the work to be performed (Services) by Microsoft (“us,” “we”) for CUSTOMER NAME REMOVED (“CUSTOMER NAME REMOVED ”, “you”, “your”) relating to the Cybersecurity Response Program (“program”).

This SOW and the associated Work Order expire 30 days after their publication date, unless signed by both parties or formally extended in writing by Microsoft.

This SOW, along with the individual projects provide a complete view of the program, and do not stand in isolation.

Common Terms and Abbreviations

The following terms and abbreviations may be used throughout this document.

Table 1: Common Terms and Abbreviations

|  |  |  |
| --- | --- | --- |
| Abbreviation | Term | Description |
| HVA | High Value Asset | Refers to a system, resource or proprietary process that if compromised would cause serious risk and business harm to the organisation. |
|  | Compromise | Refers to a system or set of systems that are no longer trustworthy to an enterprise as they are under the full control of an active adversary. |
|  | “Data” | Refers to the collected Windows Event Log, Registry Trace Logs, Windows System DLL and/or Windows Error Reporting logs. This data is not customer related or sensitive data. |
|  | Implants | A program or script that exists on a compromised host designed to perform a specific function usually with malicious intent and unknown to the enterprise. |
|  | Backdoor | Similar to an Implant however specifically designed to allow concealed access to a compromised system by an adversary unknown to the enterprise. |
| DHA | Determined Human Adversary | Refers to an individual or group that is responsible for a targeted attack. |
| APT | Advanced Persistent Threat | An advanced persistent threat (APT) is a stealthy computer network attack in which a person or group gains unauthorized access to a network and remains undetected for an extended period. The term's definition was traditionally associated with state sponsorship, but over the last few years there have been multiple examples of non-state sponsored groups conducting large-scale targeted intrusions for specific goals. |
| IoC | Indicators of Compromise | Refers to an artefact observed on a network or in an operating system that with high confidence indicates a computer intrusion. |
|  | Malcode | “Malicious Code” term used to describe hostile code that is intended to be intrusive to a system. |
| EE | Eviction Event | Planned execution of the activities required to attempt to remove the DHA and residual implants from the target platform. |
| PAW | Privileged Access Workstation | Privileged Access Workstation (PAW) is a highly controlled and managed administrative workstation that strictly controls the specific user account (role) and the specific administrative tools to only be used form this dedication hardened system to access and manage the target server workload. |
| SZ | Secure Zone | A “Secure Zone” is a reference name that defines the compartmentalised top Organisation Unit (OU) (under the Tier 1 grouping OU) which will contain all the workload related secured Group Policy Objects (GPOs), Organisation Units (OUs), admin accounts, Server Objects and Security Groups to support the hardening of the target workload |
| ADH | Active Directory Hardening | The internally developed security administration model that deploys a structured restrictive security controls to Active Directory that is used to onboard and control roles/accounts and systems |
| GPO | Group Policy Object | A control mechanism inside Active Directory used to manage specific functions |
| T0 | Tier 0 | In any identity system this represents the top most privileged accounts (i.e Domain Administration Group) or critical systems (i.e Certificate Services or Azure AD Connect) that have control or large-scale impact to the platforms |
| T1 | Tier 1 | Sits below Tier 0 however contains the highly privileged accounts that control the actual business systems where adversaries will target to meet their objective |
| RBAC | Role Based Access and Control | Identity access model that provides only the permissions required to perform a task. Permissions are assigned to the user account specifically. |
| ATP | Advanced Threat Protection | Microsoft brand for the advanced threat protection suite of technologies |
| PIM | Privilege Identity Management | Cloud service that provide just-in-time access to a resource and removes the need for permanent standing permissions |
| PAM | Privilege Access Management | On-prem service that provide just-in-time access to a resource and removes the need for permanent standing permissions |

Introduction

After undergoing an external security assessment, CUSTOMER NAME REMOVED has identified critical and high-risk security exposures in relation to highly privileged accounts that ultimately have control of business assets. The external expert that conducted the assessment then recommended that CUSTOMER NAME REMOVED approach Microsoft to ask for expert assistance in addressing this risk exposure.

Microsoft’s methodology is informed by our own internal risk and security posture and global experience, which has been translated into the recommended practices for operating an agile and secure infrastructure capability within the modern enterprise.

To date, CUSTOMER NAME REMOVED and Microsoft have engaged through a series of workshops and working groups to both commence a tactical stream of activity and to plan a strategic engagement to address the above stated risk position. These actions can be summarised as follows:

* Immediately action the “Cybersecurity Incident Response” service, which includes the assessment of CUSTOMER NAME REMOVED’s current security position (this activity is currently underway via a Unified Support engagement), which will then inform the appropriate short-term tactical Compromise Recovery actions needed by the bank;
* Propose a medium-term strategic engagement to effectively re-establish CUSTOMER NAME REMOVED’s Security and Identity foundations across critical assets and identities; and
* Develop a longer-term roadmap to further integrate Microsoft’s security and identity recommended practices across the enterprise.

The above mentioned medium-term strategic engagement plan is referred to as the Cybersecurity Response Program (CRP), which spans approximately 12 months. The CRP is the focus of this Statement of Work (SOW).

The CRP aims to significantly improve the Security and Identity foundations for the use of key elements of the Microsoft's technology platform within CUSTOMER NAME REMOVED, by leveraging Microsoft's recommended practices, most recent technology capabilities and proprietary Intellectual Property (IP).

The CRP solution addresses current critical gaps, by uplifting the Security and Identity foundations related to the Microsoft platform through the following solution areas:

* Attack Detection;
* Critical Mitigations;
* Privileged Access Security;
* Threat Detection;
* Operational Readiness; and
* Roadmap and Planning.

The CRP will effectively assist the bank in taking back control of the related privileged access management processes. This will be achieved through the following program outcomes:

* Establish highly protected, tightly controlled critical privileged accounts for on-premises and the cloud;
* Significantly reduce the risk exposure of the top privileged accounts that control the infrastructure that runs CUSTOMER NAME REMOVED’s business;
* Assist CUSTOMER NAME REMOVED with establishing their operational readiness to effectively incorporate the new security and identity management practices delivered through the CRP; and
* Assist with the initial implementation of the foundational Credentials Theft Mitigations and methodologies, with an initial focus on protecting high-value assets, that will then extend over time to the full enterprise.

This approach addresses the critical risks upfront and provides the mechanisms to progressively reduce the overall risk profile for CUSTOMER NAME REMOVED.

This SOW details the services Microsoft will provide CUSTOMER NAME REMOVED in delivering the CRP, together with the Program governance approach that ensures that the various project streams will be effectively and efficiently managed inclusive of key dependencies.

# Program objectives and scope

## Objectives

This Cybersecurity Response Program is designed to improve the Security and Identity foundations and surrounding systems related to the Microsoft technology platform, to ensure that CUSTOMER NAME REMOVED’s use of this platform is based on the latest Cybersecurity guidelines and is resilient to Credential Theft.

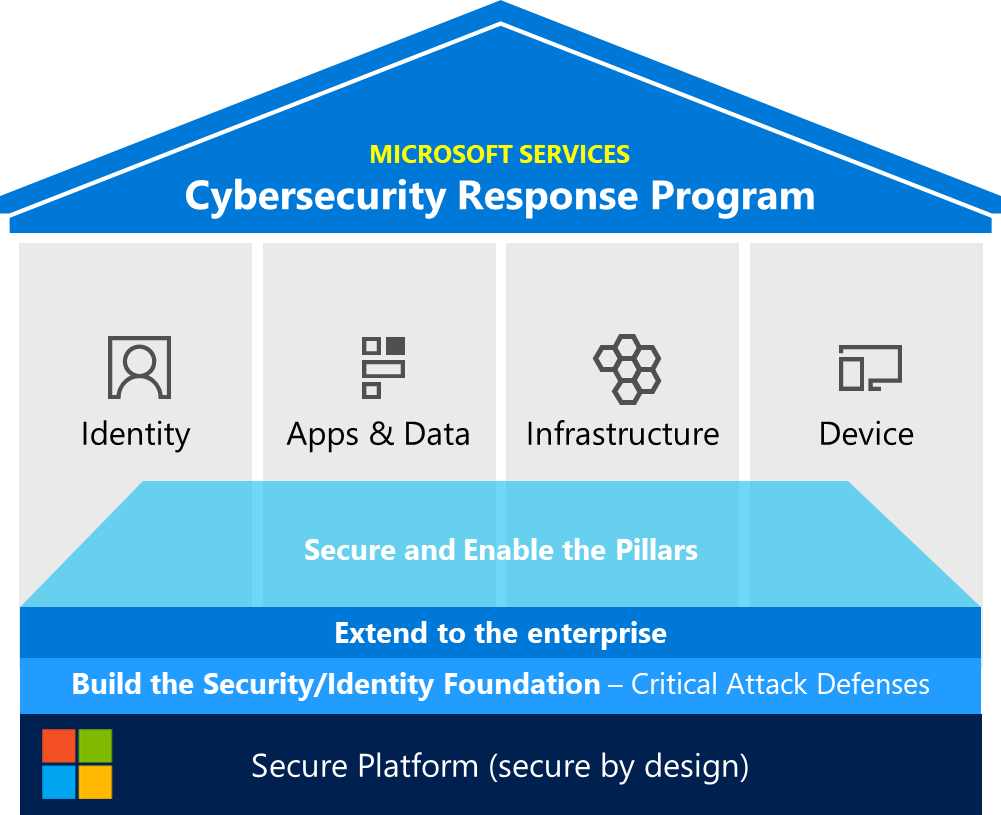


Figure 1 - Microsoft Cybersecurity Response Program

The solution delivered within the program consists of the following capabilities:

* Help in protecting an identity platform from advanced cyberattacks; and
* Securing privileged access workstations from advanced cyberattacks.

Each of these capabilities is associated with a project addressing specific requirements.

* **Attack Detection** Hunt for hidden persistent adversaries and implement critical attack detection.
* **Critical Mitigations** Critical attack protections across critical systems, highly privileged accounts and foundation endpoint security and patching.
* **Privileged Access Security** Industrial Grade protections for critical identities and assets on-premises and the cloud.
* **Operational Readiness** Assess current operational and support processes/practices for risk exposure and assist with integrating recommended practices for Credential Theft Mitigations.
* **Threat Detection** Deep analytical expertise and unique technical and human insights into threats.
* **Roadmap and Planning** Cybersecurity Architects provide recommendations and guidance reflecting the CUSTOMER NAME REMOVED landscape on attacks and strategies, build a tailored roadmap to defend your organisation’s business value and mission.

## Outcomes

This program will deliver the following outcomes:

* Significantly improved controls related to critical privileged accounts for on-premises and the cloud;
* Significantly reduced exposure of the top privileged accounts;
* Operational readiness pertinent to your operating model, incorporating security practices with critical identities; and
* Implementation of the foundation Credential Theft Mitigations and methodologies that will then progressively extend to the full enterprise.

## Areas in scope

### General program scope

The following table outlines the services that are included in this program, the program name and number under which they’re delivered in and defined in more detail.

Table 2: General program scope

|  |  |
| --- | --- |
| Project name | Description |
| P01: Active Directory Hardening (ADH) | * Active Directory Hardening is designed to address two key security gaps as follows:   + - Assess and analyse privileged account exposure and provide a migration plan for deviations from Microsoft security recommendations; and     - Deploy the Microsoft Security Administration model to the target Active Directory. * Active Directory Hardening utilises enhanced technologies and recommended practices to provide enhanced security protection and security controls to:   + - Tier 0 (highly privileged top-level accounts);     - Tier 1(server workload privileged accounts); and     - Tier 2 (privileged accounts for support desk operations). * Active Directory Hardening will focus on Tier 0 only in this scope and be deployed for up to ten (10) Active Directory domains. * Provide support and guidance to the AD consolidation teams with a focus on technical requirements, supported configuration patterns, operational risks and guidance on migration practices and processes to consolidate Active Directory domains. |
| P02: Enhanced Security Administrative Environment (ESAE) | Enhanced Security Administrative Environment (ESAE) provides advanced protections for Tier-0 highly privileged top-level accounts (Domain Administrators, Enterprise Administrators, and equivalent) based upon Microsoft’s recommended practices and accumulated field experience.  ESAE helps protect these Tier-0 accounts with dedicated administrative workstations, enhanced hardened security controls and configurations, and a dedicated environment to administer identity within the organisation.  CUSTOMER NAME REMOVED has identified ten (10) Active Directory domains of critical importance and has indicated that a consolidation is complex and is currently being assessed. Therefore, in order to support the protection of these critical accounts the Enhanced Security Administrative Environment (ESAE) will be deployed for up to ten (10) domains to take control of these privileged accounts. |
| P03: Privileged Access Workstation (PAW) – Tier 1 | Once Tier 0 is under control and protected the program will shift focus to Tier 1. This Tier, although less privileged then Tier 0, is still critical as this is the set of privileged accounts that are operating and control CUSTOMER NAME REMOVED’s business systems. Attackers will target Tier 1 systems in the event they can’t access the top-level Tier 0 accounts.  This project focuses on three major outcomes:   * Assess and adapt the Microsoft Active Directory Administration Model specifically to provide security controls and hardening restrictions to the Tier 1 server workloads (not the installed applications, only the server OS). * Deploy a Privileged Access Workstation (PAW) specific to that workload(s) to protect the privileged credentials that are used to manage the workload. * Assess and deploy Privileged Access Workstations (PAW) to be used in conjunction with the inflight PAM platform as the trusted administrative source (clean keyboard model).   + Up to ten (10) workloads are in scope, it is assumed that of these ten (10); five (5) will be standalone agreed upon high value assets and the remaining five (5) are Privileged Access Workstations (PAW)s configured to work in conjunction with the in-flight PAM solution.   Privileged Access Workstation (PAW) is a highly controlled and managed administrative workstation that strictly controls the specific user account (role) and the specific administrative tools to only be used form this dedication hardened system to access and manage the target server workload. This hardening and control are part of the Microsoft Active Directory Administration Model set of controls.   * Support CUSTOMER NAME REMOVED with the expansion of the Tier 1 administrative security model that consists of secured Group Policy Objects (GPOs), Organisation Units (OUs), and Security Groups to provide a compartmentalisation model (Secure Zone) to: * Apply restrictive security controls to the Windows Server OS of the target workload; * Support the deployment of a PAW for administration of the target workload; * Support the Implementation up to ten (10) Tier 1 secure zones to harden a High Value Asset workload per zone (either stand alone or in conjunction with the PAM solution); * Reduce the risk of administrative credential theft by reducing the exposure of administrative workstations through the deployment of Privileged Access Workstations (PAW)s; * This scope covers:   + - Implementation of up to ten (10) PAW workstations, one (1) per Secure Zone.     - Implementation of up to two (2) administrative applications per security zone. |
| P04: Azure Security Foundations | Cloud identities are just as critical and vulnerable to attack as the identities on-premises. Managing the identities for any cloud workload is the last mile responsibility of CUSTOMER NAME REMOVED as such due diligence to wrap the same security controls and restrictions to these highly privileged accounts is critical.  CUSTOMER NAME REMOVED has an extensive Azure deployment and existing Role Based Access (RBAC) model to manage identities in the Azure platform. This project is focused only on the highest privileged credentials that sit atop this existing RBAC model.  Design and build the component services and features that will support a robust security protection of cloud-based identities and Azure platform focused on the core privileged identities that manage and control the cloud platform.   * The component services and features to achieve this are:   + - Role Based Access Control (RBAC);     - Azure Identity Protection;     - Azure Privilege Identity Management; and     - Conditional Access. * This scope covers:   + - up to six (6) separate Azure tenants, each with up to one (1) subscription per tenant. |
| P05: Azure Cloud PAW | As with the Privileged Access Workstation (PAW), similar cloud controlled, and managed administrative workstations are used to protect the top privileged accounts that control Azure cloud deployments. Cloud PAW leverages the same reference architecture as the on-premises version; however, it is fully managed and controlled by Azure security features and controls. This gives an administrative and security boundary to these cloud-based admin accounts.   * Cloud PAW reduces the risk of cloud privileged administrative credential theft by reducing the exposure of administrative workstations. * Implement Cloud PAWs with applications for the following administrative tasks, which are based on Microsoft-recommended practices, architectures, accumulated field experience:   + - Azure Active Directory;     - Azure Administrative Portal; and     - Office 365 Administrative Portal. * Cloud PAW leverages the most advanced security features in the Azure Security and Windows 10 Enterprise, including:   + - Unified Extensible Firmware Interface (EFI) Secure Boot     - Windows BitLocker Drive Encryption     - Windows Defender Antivirus     - Windows Defender Credential Guard     - Windows Defender Exploit Guard     - Windows Defender Firewall     - Windows Defender Application Control (WDAC)     - Integration with Azure Log Analytics     - Intune compliance and configuration policy     - Azure Active Directory Conditional Access     - Windows Defender ATP     - Azure Active Directory Identity Protection     - Azure Active Directory PIM     - Azure Active Directory Delegation of Admin design * This scope covers:   + - Up to six (6) separate Azure tenants, each with up to one (1) subscription per tenant are in scope.     - Up to six (6) Azure Cloud PAW’s are in scope. |
| P06: Advanced Threat Detection Implementation Service (ATDIS) | In discussions between CUSTOMER NAME REMOVED and Microsoft it has been identified that the capability to detect credential theft attempts is currently limited and is an area of critical importance to a strong security posture.  CUSTOMER NAME REMOVED has a significant presence across Azure and Office 365 along with a significant fleet of end user and server systems. The use of the ATP security suite of detection tools allows CUSTOMER NAME REMOVED to have an early signal, backed by AI, to detect a breach attempt and move to a model that can operationalise incident response when it happens.  This project designs and implements:   * + - Azure Advanced Threat Protection or Advanced Threat Analytics;     - Office 365 Advanced Threat Protection; and     - Windows Defender Advanced Threat Protection.   These components provide threat protection and detection services across multiple attack surfaces:   * + - Active Directory Domain Services, Azure virtual machines and web applications, Windows devices and Office 365 services.     - Provide an understanding of the threats that Windows Defender will block or mitigate.     - Provide an understanding of the threats for which Azure Advanced Threat Protection, Office 365 Advanced Threat Protection and Windows Defender Advanced Threat Protection will generate alerts.     - Assist with the creation of a response activation worksheet that is specific to the events that Azure Advanced Threat, and Windows Defender Advanced Threat Protection detect.     - Assist with the design and implementation of Azure Advanced Threat Protection to monitor for threats to CUSTOMER NAME REMOVED’s production Active Directory Domain Services (AD DS) environment. * This scope covers:   + - Up to two (2) AD DS forests     - Up to one (1) Azure subscription     - Up to one (1) Office 365 tenant. |
| P07: Modern Desktop Deployment | Advanced Persistent Threats (APTs) have used OS deployment and management tools of all brands to package and distribute malware inside of organisations. This type of persistence is easily accomplished as typically these OS management platforms have some form of administrative access to large quantities of systems and are deemed to be trusted.  This project focuses on gaining control of the privileged accounts that manage the System Center deployment platform for Windows end user computing (which often include administrator systems). This project assumes the current platform is untrusted and builds the base system from known good media and a trusted keyboard.   * Design and deploy a distinct System Center Configuration Manager (SCCM) deployment infrastructure for Windows 10 current branch. * Implement a secured Tier 1 Role Based Access and Control (RBAC) model for roles that require the permission to “create” or “edit” an automation sequence or any privileged administrative function of the SCCM infrastructure. * Implement a secured and isolated Tier 2 Role Based Access and Control (RBAC) model for roles that require the permission to “execute” an automation sequence for OS deployment. * Implement the following security functionality into the Windows 10 OS:   + - BitLocker: basic unlock method, recovery key backup to Active Directory Domain Services (AD DS), operating system drive, and removable media encryption;     - Credential Guard: implementation of the feature;     - User Account Control: implementation of the feature;     - Windows Defender: scan, signature update, Microsoft Active Protection Service, real-time scan, quarantine, and implementation policy;     - SmartScreen: implementation of the feature in Windows, Microsoft Edge, and Internet Explorer; and     - Security Baseline: application of the baseline security controls to the devices based on the Microsoft Security Compliance Manager and the Australian ISM Manual. * This scope covers:   + - One (1) primary site     - Up to five (5) distribution points     - One (1) reporting point |
| P08: Modern Server Deployment | Building on the Modern Desktop Deployment project above, this project focuses on gaining control of the privileged accounts that manage the System Center deployment platform for Windows Server deployments. This is critical as most organisations will leverage a hypervisor platform and will have “golden images” that are copied over and over each time a server workload is required to be built. Leveraging a deployment platform protects the source image from being corrupted by and APT and allows a trusted server image to be deployed repeatedly.  This project assumes the current platform is untrusted and builds the base system from known good media and a trusted keyboard:   * Design and deploy a distinct System Center Configuration Manager (SCCM) deployment infrastructure for Windows Server 2016; * Implement a secured Tier 1 Role Based Access and Control (RBAC) model for roles that require the permission to “create” or “edit” an automation sequence or any privileged administrative function of the SCCM infrastructure; * Implement a secured and isolated Tier 2 Role Based Access and Control (RBAC) model for roles that require the permission to “execute” an automation sequence for OS deployment. * Implement the following security functionality into the Windows Server 2016 OS:   + - Security Baseline: application of the baseline security controls to the devices based on the Microsoft Security Compliance Manager, Enhanced Mitigation Experience Toolkit (EMET) controls and the Australian ISM Manual. * This scope covers:   + - One (1) primary site     - Up to five (5) distribution points     - One (1) reporting point |
| P09: Operational Service Management | The security controls introduced in this program of work, will change the way IT administers the various critical systems and the privileged accounts that control them.  This project is specifically designed to support CUSTOMER NAME REMOVED in understanding, adapting and operationalising the security practices that are being introduced, by:   * Discover and Analyse existing Admin Credential Support Practices and Tools   + - Assess current support processes and practices for risk exposure, and assist with integrating recommended practices into IT system administration and maintenance of PAW solution for Tier 1 and Azure Cloud; and     - Assess current support processes and practices for risk exposure and assist with integrating recommended practices into IT system administration and maintenance of the ESAE solution. * PAW Tier 1 and PAW Azure Cloud Support Roles and Process determination   + - Define Server support requirements and processes for Tier 1 and Azure Cloud.   Operations, Maintenance and integration Planning.   * Plan PAW Tier 1 and PAW Azure Cloud support and operations integration into CUSTOMER NAME REMOVED’s existing Change, Configuration, Incident and Event Management processes. Create PAW Tier 1 and PAW Azure Cloud User and Admin Management Plan. * Plan ESAE support and operations integration into CUSTOMER NAME REMOVED’s existing Change, Configuration, Incident and Event Management processes. * Plan ATP (Azure, O365 and AD) support and operations integration into CUSTOMER NAME REMOVED’s existing Change, Configuration, Incident and Event Management processes. * Assess, modify and implement the Windows 10 servicing update management. * Assess, modify and implement the Windows Server servicing update management. |
| P10: Adoption and Change Management Assistance | * Four (4) week engagement in which an ACM specialist will provide guidance on adoption and change management to CUSTOMER NAME REMOVED as it relates to the solution being deployed by this program. |

### Software products and technologies

The software products and technologies required for each project are defined within their respective project section.

**Important Note:** Microsoft as part of this program will install software during the build phase of required projects. CUSTOMER NAME REMOVED temporarily appoints Microsoft to act as its agent for the limited purpose of accepting and agreeing to the user terms of any click-through license agreement which accompanies the software (Microsoft or non-Microsoft) which is listed in this SOW and is included within the test and development environments. CUSTOMER NAME REMOVED can read these terms 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 Project Manager.

Unless otherwise agreed to in writing CUSTOMER NAME REMOVED temporarily entitles Microsoft to act as its agent for the download of the required software. With this authority, Microsoft can apply the known-good media process to download and validate the required software and can compile the software into a specific disk image structure which can be used to build an MDT server or provide a known good build ISO image.

## Areas out of scope

Any area not explicitly included in the Areas in scope section is out of scope for Microsoft during this program. Specific areas out of scope for this program are listed in the following table.

Out of scope items specific to an individual project can be found within the out of scope section of that specific project.

Table 3: General program out of scope

|  |  |  |
| --- | --- | --- |
| Area | Description | |
| Business process reengineering | Designing functional business components of the Solutions are not included. |
| Data migration | Data migration activities are not in scope for this program. |
| Hardware | Microsoft will not provide hardware for this program. |
| Integration with third-party software | Microsoft will not be responsible for integration with third-party software. |
| Organisational change management | Designing—or redesigning—CUSTOMER NAME REMOVED’s functional organisation is not included. |
| Product bugs  and upgrades | Product upgrades, bugs, and design change requests for Microsoft products are not in scope for this project. |
| Product licenses and subscriptions | Product licenses (Microsoft or non-Microsoft) and cloud service subscriptions are not included.  Procurement of required server licenses or client access licenses, including external connectors, is out of scope. |
| Review and certification | Review, analysis or certification of recommended practice of any deliverable not developed by Microsoft Services are not included. |
| Source code review | CUSTOMER NAME REMOVED will not provide Microsoft with access to non-Microsoft source code or source code information. For any non-Microsoft code, Microsoft Services will be limited to the analysis of binary data, such as a process dump or network monitor trace. |
| System integration | System integration and interfaces are not in scope. |
| Third Party Management | Management of third party or CUSTOMER NAME REMOVED resources or tasks. |
| Formal training | Formal classroom or hands-on lab training, unless otherwise specified in a project. | |
| Managed Services | Ongoing operational management of any solution deployed during this program. | |
| Support | Post deployment support. Additional support can be purchased separately. | |
| Current Production environment | Changes to the current environment to resolve problems not related to the defined scope of this project are out of scope. | |
| Test environment | * Building of a test environment. * Duplication of CUSTOMER NAME REMOVED ’s existing Windows corporate domain environment within a test lab or the creation of CUSTOMER NAME REMOVED‘s test domains to simulate production domains. * Running of test cases. | |
| System runbooks and playbooks | * Preparation of system runbooks and playbooks. | |
| Networking services | * Setup or configuration of network load-balancing servers or services, including more secure reverse proxy publishing mechanisms. | |
| Monitoring services | * Setup or configuration of monitoring, auditing, or alerting services to monitor the health of the environment beyond any items that are explicitly included in the scope. | |
| Migration or consolidation | * Migration, consolidation, or rationalisation of AD DS objects, including users, groups, workstations, servers, applications, or group policies—this includes logon scripts and data migration. | |

# Program approach, timeline, and deliverables

## Approach

This program consists of ten distinct Projects, each with its own objective, activities, scope and deliverables. These projects are defined in this SOW from Section 5 onwards.

The Projects that form this overall program are:

* P01: Active Directory Hardening (ADH)
* P02: Enhanced Security Administrative Environment (ESAE)
* P03: Privileged Access Workstation (PAW) – Tier 1
* P04: Azure Security Foundations
* P05: Azure Cloud PAW
* P06: Advanced Threat Detection Implementation Services (ATDIS)
* P07: Modern Desktop Deployment
* P08: Modern Server Deployment
* P09: Operational Service Management
* P10: Adoption and Change Management Assistance

Microsoft uses proven delivery methodologies uniquely suited for delivery of Microsoft Services relevant to the technologies being designed and deployed or being adopted by CUSTOMER NAME REMOVED. For this program, Microsoft will use a combination of delivery methodologies, each suited for the scope of services provided in the respective project. The Project Manager will establish the overall governance framework for the program as well as set recommended practices and uniformity across projects. Please refer to the Project section for individual project details and the specific methodology to be used.

Our program governance follows defined phases to initiate, plan, execute, control, and close the program. The program governance will involve definitive phases that have specific deliverables and activities. The following are the key phases of the program:

* Initiating: program introduction, draft governance documentation;
* Planning: finalise all management plans, set up governance boards;
* Executing: manage program-level tasks according to governance documentation;
* Controlling: manage scope, schedule, financials, quality, risks/issues, performance, staffing and reporting metrics across the program; and
* Closing: facilitate transition to operations, conduct closure.

Within this delivery management framework, each project will be executed following the high-level overview illustrated in the Program objectives and scope section. More details for each phase are provided in the sections below.

### Program dependencies

Some of the projects included in this program have dependencies on one another. A high-level overview of these dependencies is outlined in the table below. The projects listed in the “Dependency” column, if any, must be completed in part or in their entirety before the project listed in the first column begins. The program scope, schedule or cost may be impacted if these dependencies are not satisfied.

Table 4: Program dependencies

|  |  |
| --- | --- |
| Project | Dependency |
| Privileged Access Workstation Tier 1 | Active Directory Hardening |
| Azure Security Foundations | Azure Cloud PAW |
| Modern Desktop Deployment | Active Directory Hardening |
| Modern Desktop Deployment (Production Build) | Privileged Access Workstation Tier 1 (SCCM Workload) |
| Modern Server Deployment | Active Directory Hardening |
| Modern Server Deployment (Production Build) | Privileged Access Workstation Tier 1 (SCCM Workload) |

### Program initiation

During the Initiating phase, the Program and Project Manager reviews the project documents to align expectations between the program/project teams and stakeholders. This phase indicates that the team is aligned to a common vision and the specific scope of work necessary to bring the vision to reality. Successful delivery and adherence to the schedule defined in this approach section requires CUSTOMER NAME REMOVED to complete the CUSTOMER NAME REMOVED activities prior to program kick-off.

Any prerequisites unique to a project can be found in the project initiation details for that project.

Table 5: Program initiation activities

|  |  |  |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | * Work with CUSTOMER NAME REMOVED to understand and document key stakeholder relationship map and stakeholder matrix. * Review schedule and validate WBS. * Establish core team (Project Manager, Domain Solution Architect, Account Delivery Executive). * Draft program management plan, including schedule, financial, quality, deliverable and communication plans. * Set up SharePoint site as team workspace for collaboration (or use a CUSTOMER NAME REMOVED supplied site if one is established by CUSTOMER NAME REMOVED). * Establish relationship with CUSTOMER NAME REMOVED and establish Conditions of Satisfaction (CoS). * Conduct delivery on-boarding meeting. * Conduct a detailed walk-through of the SOW with the CUSTOMER NAME REMOVED and Microsoft teams. * Establish deliverables tracking. * Track the status of kick-off prerequisites and adjust the program initiating phase start date accordingly. * Deliver program kick-off to all stakeholders. |
| **CUSTOMER NAME REMOVED activities** The activities to be performed by CUSTOMER NAME REMOVED | * Communicate internal (and partner) stakeholder names to the Microsoft Project Manager. * Assist with key stakeholder introductions and mapping. * Review schedule, staffing, financial, deliverable and Program Management Plans. * Provide access to key information regarding current processes and tools. * Assign project initiation and kick-off prerequisite responsibilities to accountable leadership and establish target completion dates. * Staff the project with the required resources in the mutually agreed time frames. * Assist in preparing and delivering program/project kick-off meeting, schedule the meeting and participate. * Provide requirements for collaboration or provide access to existing CUSTOMER NAME REMOVED SharePoint site. * Align business strategy, with clear strategic concepts related to starting Program. |

### Program planning

During the planning phase, the major activities include review of the overall schedule, creation of an integrated master schedule, and agreement on reporting and governance standards such as the program management plan.

Table 6: Program planning activities

|  |  |  |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | * Create integrated master schedule. * Finalise and publish program management plan. * Update risk and issue log. * Review project requirements, methodology details, workshops, iterations. |
| **CUSTOMER NAME REMOVED activities** The activities to be performed by CUSTOMER NAME REMOVED | * Provide contact, email, and organisational title information for key stakeholders and review areas of interest. * Review high-level architecture. * Review/approve integrated master schedule. * Review/approve program management plan. * Identify team members to participate in the Executive Steering Committee. |
| Key assumptions | * Program documentation will undergo periodic review. |

### Program executing and controlling

Program executing and controlling spans from planning through to closing. During executing, the major program management activities include updates to the solution design and governance standards, monitoring progress of the projects and facilitation of the Executive Steering Committee. More details on the governance processes can be found in the Program governance section and details for the delivery of each project can be found in the relevant project section.

Table 7: Program executing and controlling activities

|  |  |  |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | **Execute**   * Facilitate Executive Steering Committee. * Execute program management plans. * Review end-to-end solution design. * Review and revise program management plans, as needed. * Quality control – delivery and documentation. * Capture lessons learned. * Review and refine resource plan, as needed (submit requests, adjust budget and forecast). * Conduct one-hour assessment workshop to assess CUSTOMER NAME REMOVED readiness to operate the solution. * Obtain sign-off, go/no-go decisions as required.   **Control**   * Manage key elements of program, including roll-up and consolidation of status, scope, schedule, cost, risks/issues, staffing and performance. * Manage executive stakeholder relationships. * Report performance against Conditions of Satisfaction (COS). |
| **CUSTOMER NAME REMOVED activities** The activities to be performed by CUSTOMER NAME REMOVED | * Organisation and/or adoption change management plans. * Validate that key stakeholders participate in Executive Steering Committee. * Provide representation in ARB (Architecture Review Board). |
| Key assumptions | * All stakeholders, including IT, business and end users agree on definition of success. * Deployment metrics are tracked according to pre-approved measures. |

### Program closing

The program will undergo a formal close process as follows:

Table 8: Program closing activities

|  |  |  |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | * Execute transition to support plan. * Conduct final lessons learned. * Conduct final knowledge transfer to CUSTOMER NAME REMOVED, operations and support teams. |
| **CUSTOMER NAME REMOVED activities** The activities to be performed by CUSTOMER NAME REMOVED | * Participate in transition to CUSTOMER NAME REMOVED support. * Compare outcomes with expectations and provide feedback. * Verify all deliverables have been signed off. * Participate in lessons learned. * Provide resources for knowledge transfer. |

## Program timeline

During planning of the program, a detailed program timeline will be developed. All dates and durations shown in the figure below are relative to the program start date and are estimates only.

The Microsoft Program Manager, Project Manager and Architect should be established no later than two (2) weeks before the start of the first project. This allows the stakeholders to become acquainted with the processes, communication rhythm and tools planned for the reporting of status, issues/risks, financials & deliverables.

It is estimated that the program will be performed per the timeline depicted below. Each project will be delivered in the approximate sequence shown. The detailed timeline for each can be found in the relevant project section.

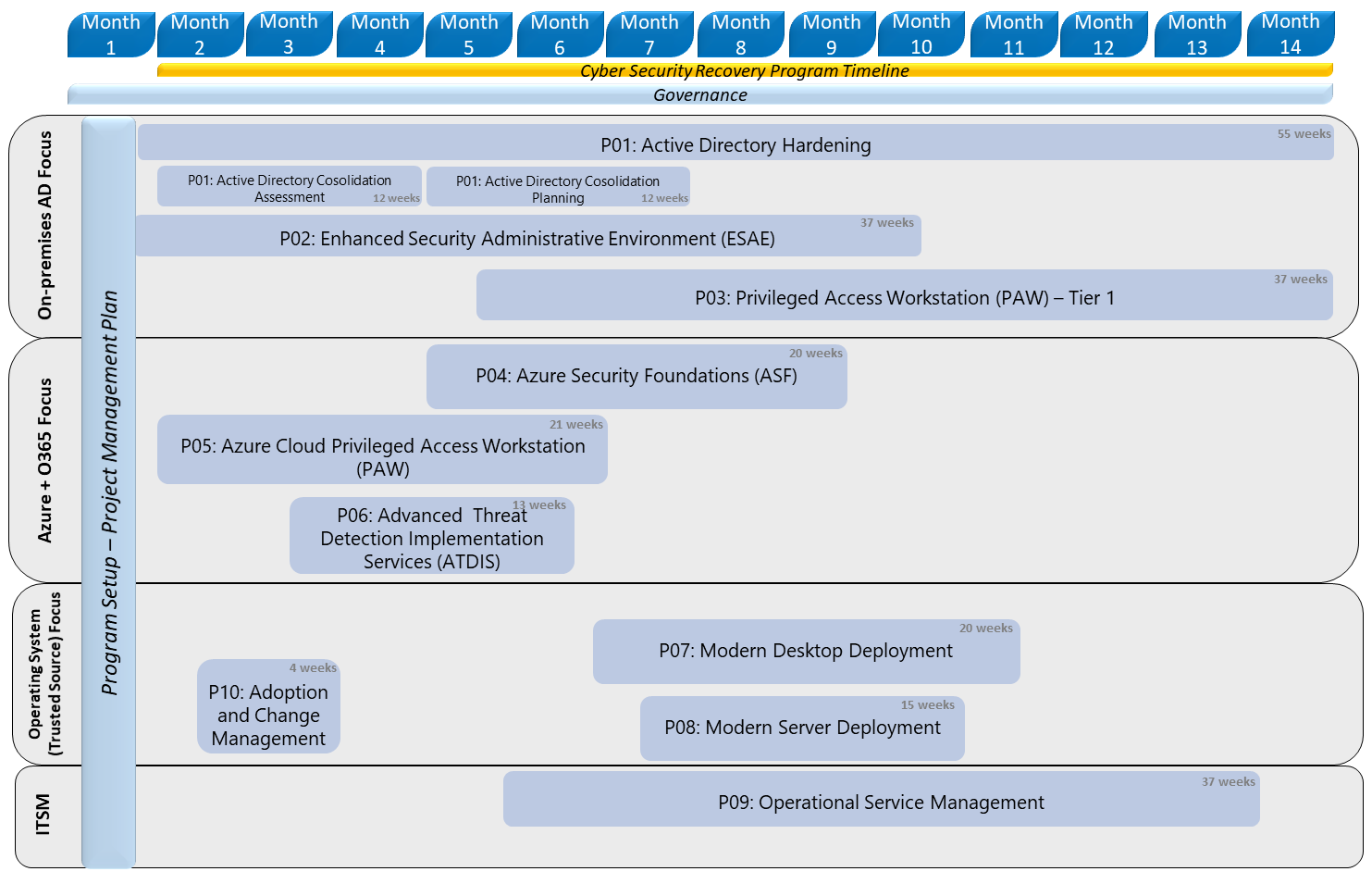


Figure 2: Program Timeline

## Program Pre-Requisites / Dependencies

The following pre-requisites and dependencies are required before the start of each project. Any delay in providing the items in the table below may have an impact to the project start.

Table 9: Program Pre-Requisites/Dependencies

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Project | Dependency name | Dependency description | Responsibility |
| PR01 | P03 PAW – Tier 1 | Secure Room | Required for Microsoft/CUSTOMER NAME REMOVED resources to reside | CUSTOMER NAME REMOVED |
| PR02 | P02 – ESAE  P03 – PAW – Tier 1 | Secure Laptops | Required for secure workstation build (CUSTOMER NAME REMOVED resource use) | CUSTOMER NAME REMOVED |
| PR03 | Program | Independent Internet | A public internet that is not connected to CUSTOMER NAME REMOVED network as part of Cyber protocol | CUSTOMER NAME REMOVED |
| PR04 | Program | Privileged Accounts | Access to be provided for specific users to privileged accounts | CUSTOMER NAME REMOVED |
| PR05 | P05 Cloud PAW | E5 Licenses | For Cloud PAW administrators only | CUSTOMER NAME REMOVED |
| PR06 | P02 ESAE | Server build | Servers to be built for ESAE Red Forest platform – physical or virtual (number to be defined during design) | CUSTOMER NAME REMOVED |
| PR07 | P01 ADH | Firewall changes | Firewall changes and ports to be opened for AD/Domain Controllers to communicate freely with CUSTOMER NAME REMOVED’s servers and desktops – to allow GPO push. | CUSTOMER NAME REMOVED |
| PR08 | P05 ATDIS | SIEM integration | CUSTOMER NAME REMOVED will be required to integrate ATDIS Event Hub into SIEM | CUSTOMER NAME REMOVED |

## Program deliverables

This section provides a list of the deliverables produced at the program level. If a deliverable requires formal review and acceptance (indicated by a Yes), it will be governed by the deliverable acceptance process as defined in section 2.5.

Table 10: Program deliverables

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Phase | Deliverable name | Deliverable description | Acceptance required? | Responsibility |
| D01 | Program initiation | Draft program management plan | Microsoft Word document with a detailed description of how the program will be managed, including communication, change, deliverable, financial, quality, risk, schedule, scope management. | No | Microsoft |
| D02 | Program initiation | Program kick-off presentation | PowerPoint slides to introduce the program, projects, governance approach and timeline. | No | Microsoft |
| D03 | Program Planning | Final program management plan | Microsoft Word document with a detailed description of how the program will be managed, including communication, change, deliverable, financial, quality, risk, schedule, scope, staffing, security, test management. | No | Microsoft |
| D04 | Program Planning | Cybersecurity Architecture Gap Analysis report | A Microsoft Word document (up to 20 pages) summarising the analysis of gaps in the current cybersecurity architecture based on Microsoft-recommended practices | No | Microsoft |
| D05 | Program Closure | Cybersecurity Architecture Summary | A Microsoft PowerPoint summary (up to 20 slides) with the modernised cybersecurity architecture | No | Microsoft |

## Deliverable acceptance process

During the program, Microsoft will submit certain deliverables for CUSTOMER NAME REMOVED’s review and approval. The deliverables which require formal acceptance are specified with Acceptance Required “Yes”.

Items that do not require acceptance are considered Work Products and do not require formal acceptance.

Within three (3) business days of the date of submittal, CUSTOMER NAME REMOVED is required to:

* **Accept the deliverable** by signing, dating, and returning a service deliverable acceptance form, which can be sent by email, or by using (or partially using) the deliverable

Or

* **Reject the deliverable** by notifying Microsoft in writing; CUSTOMER NAME REMOVED must include a complete list of reasons for rejection.

Or

* **Escalate:** If either Microsoft or CUSTOMER NAME REMOVED are unable to agree on accepting the Deliverable or on the feedback received in rejecting the Deliverable and/or its resolution, then either party may escalate the issue as detailed in the Escalation path section.

Deliverables shall be deemed accepted after three (3) days unless the written rejection notification is received by Microsoft in the timeframe specified.

If a rejection notification is received, Microsoft will correct problems with a deliverable that are in scope for the program (and documented in this SOW or the projects in the Project section), after which the deliverable is deemed accepted.

Problems that are outside the scope of this SOW, and feedback provided after a deliverable has been accepted will be addressed as a change request, managed as described in the Change management process section.

## Defect remediation

As defects are identified during testing, the defect priority will be jointly agreed upon by CUSTOMER NAME REMOVED and Microsoft. The Microsoft team will triage the defect and fix all in-scope P1 and P2 defects. Defect priorities are shown in the following table.

Table 10: Defect Priorities

|  |  |  |
| --- | --- | --- |
| Priority | Description | Remediation in scope? |
| P1 | **Blocking defect**  Development, testing, or production launch cannot proceed until this type of defect is corrected. A defect of this type blocks further progress in this area. The solution cannot ship, and the project team cannot achieve the next milestone until such a defect is corrected. | Yes |
| P2 | **Significant defect** This type of defect must be fixed prior to moving to production. Such a defect, however, will not affect test plan implementation. | Yes |
| P3 | **Important defect** It is important to correct this type of defect. However, it is possible to move forward into production using a workaround. | No; the problem will be logged. Remediation will be performed through an agreed-upon change request only. |
| P4 | **Enhancements and low priority defects** P4 defects consist of feature enhancement and cosmetic defects. These include design requests that vary from original concepts. | No; the problem will be logged. Remediation will be performed through an agreed-upon change request only. |

## Program governance

The governance structure and processes the team will adhere to for the program are described in the following sections.

### Program communication

The following will be used to communicate during the program:

* **Communication plan**: this document will describe the frequency, audience, and content of communication with the team and stakeholders. It will be developed by Microsoft and CUSTOMER NAME REMOVED as part of program planning.
* **Program summary reports**: the Microsoft Program Manager, working in conjunction with the CUSTOMER NAME REMOVED Program Manager, will compile a program status report for distribution to the Steering Committee and both CUSTOMER NAME REMOVED and Microsoft management per the frequency defined in the communication plan.
* **Status reports**: the Microsoft Project Manager will prepare and issue regular status reports to the CUSTOMER NAME REMOVED Program Manager per the frequency defined in the communication plan.
* **Status meetings**: the Microsoft team will schedule regular status meetings to review the overall project status, the acceptance of deliverables, and review open issues and risks per the frequency defined in the communication plan.

### Program risk and issue management

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

* **Identify**: identify and document project issues (current problems) and risks (potential problems that could affect the project).
* **Analyse and prioritise** assess the potential impact and determine the highest priority risks and issues that will be actively managed.
* **Plan and schedule**: determine the strategy for managing priority risks and issues and identify a resource who can take responsibility for mitigation and remediation.
* **Track and report**: monitor and report the status of risks and issues.
* **Escalate**: escalate to project sponsors the high impact issues and risks that the team is unable to resolve.
* **Control**: review the effectiveness of risk and issue management actions.

Active issues and risks will be regularly monitored during the program. The Microsoft Project Manager is responsible for collecting and reviewing all project risks to confirm they are being appropriately managed, as well as to assess the impacts across projects. These risks will be communicated to program stakeholders during weekly program reviews and monthly Executive Steering Committee meetings.

### Change management process

During the program, either party can request modifications to the Services described in this SOW. These changes only take effect when the proposed change is agreed upon by both parties. The change management process steps are:

* **The change is documented**: all change requests will be documented by Microsoft in a Microsoft change request form and submitted to CUSTOMER NAME REMOVED. The change request form includes:
  + A description of the change.
  + The estimated effect of implementing the change.
* **The change is submitted**: the change request form will be provided to CUSTOMER NAME REMOVED.
* **The change is accepted or rejected**: CUSTOMER NAME REMOVED has three (3) business days to confirm the following to Microsoft:
  + Acceptance: CUSTOMER NAME REMOVED must sign and return change request form.
  + Rejection: if CUSTOMER NAME REMOVED does not want to proceed with the change or does not provide an approval within three business days, no changes will be performed.

### Executive Steering Committee

The Executive Steering Committee (ESC) provides overall senior management oversight and strategic direction for the program. The ESC for the program will meet per the frequency defined in the communication plan and will include the roles listed in the following table. The responsibilities for the committee include:

* Making decisions about program strategic direction.
* Serving as a final arbiter of program or project issues.
* Approving significant change requests.

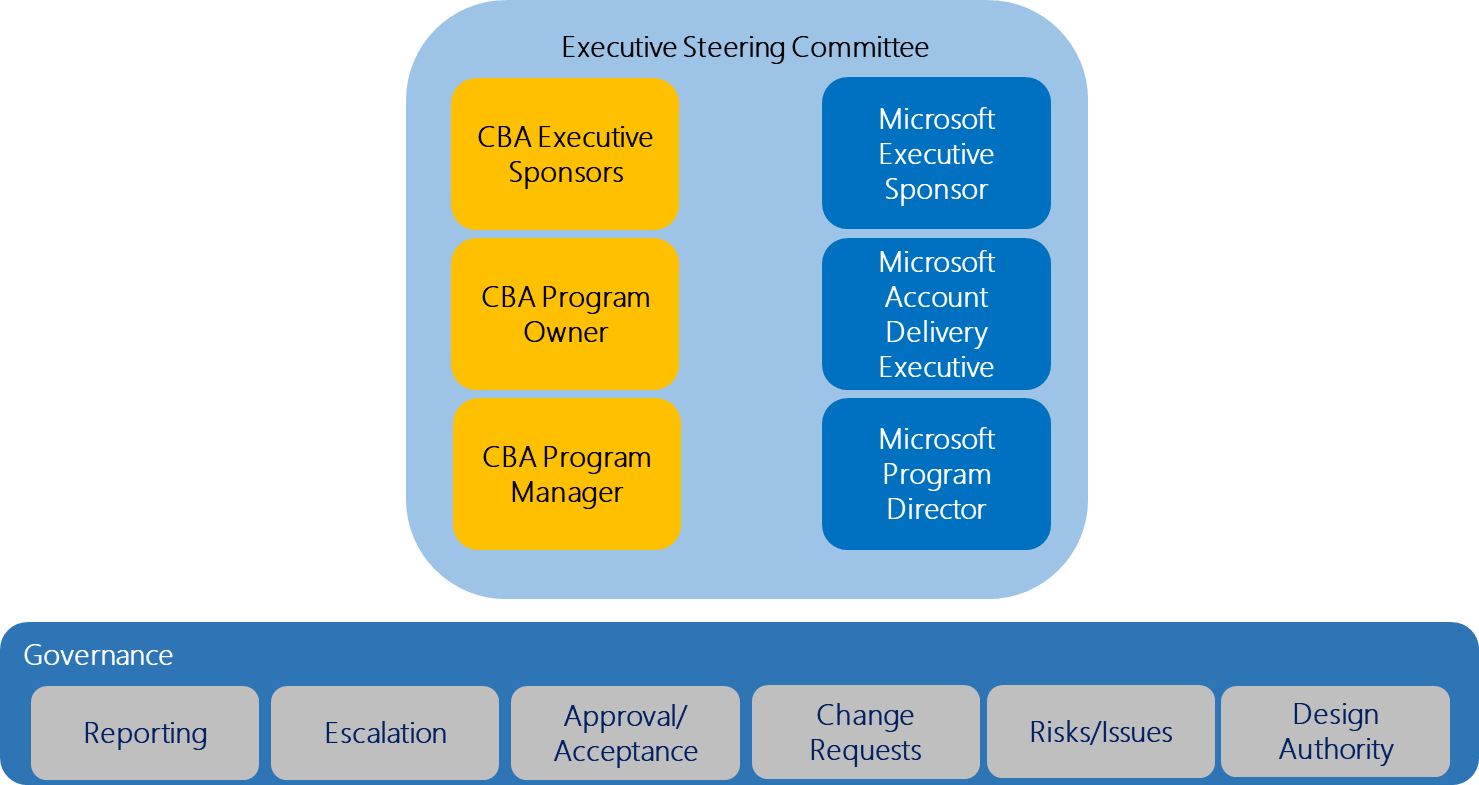


Figure 3: Executive Steering Committee (ESC)

### Escalation path

The Microsoft Project Manager will work closely with the CUSTOMER NAME REMOVED Program Manager, Sponsor, and other designees to manage issues, risks, and change requests as described previously. CUSTOMER NAME REMOVED will provide reasonable access to the sponsor, or sponsors, to expedite resolution. The standard escalation path the team will follow for review, approval, or dispute resolution is as follows:

* **Level 1: Project Manager (Microsoft and CUSTOMER NAME REMOVED)**

The Project managers are expected to resolve project and program issues. If the Project managers are unable to resolve the issue, it should be escalated to the next level.

* **Level 2: Program Director and Program Manager (Microsoft and CUSTOMER NAME REMOVED)**

The Microsoft Program Director, CUSTOMER NAME REMOVED Program Manager, Microsoft ADE and CUSTOMER NAME REMOVED Program Owner will work together to resolve issues that could not be resolved by the project manager. Any issues that cannot be resolved at this level will be escalated to the Executive Steering Committee for resolution.

* **Level 3: Executive Steering Committee (Microsoft and CUSTOMER NAME REMOVED)**

This team is the final decision maker for escalations. It is not necessary to wait for the regularly scheduled ESC meeting to raise escalations.

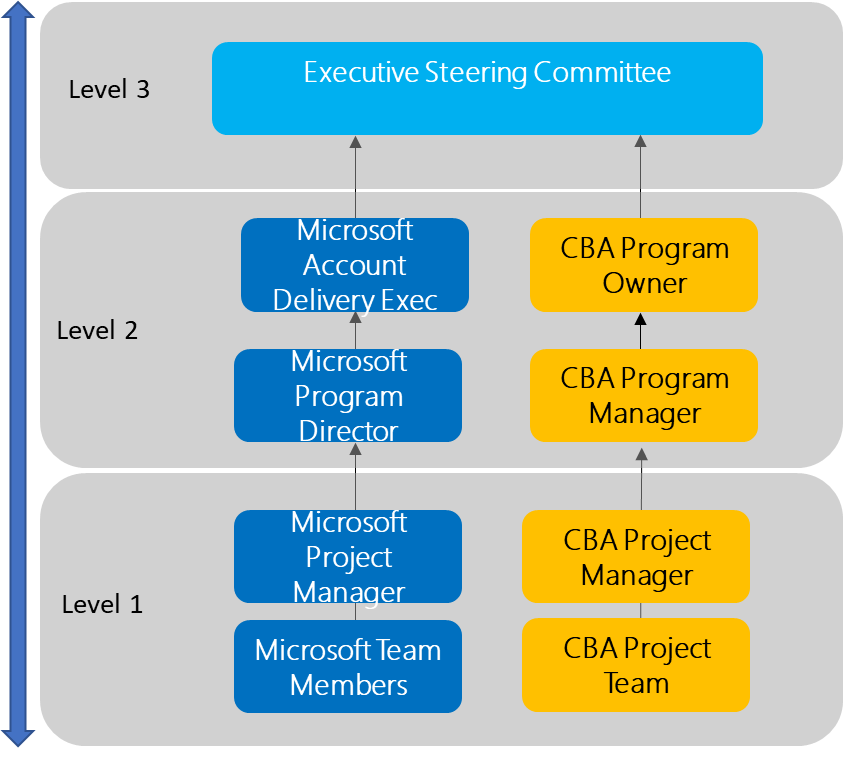


Figure 4: Escalation Path

### Architectural Review Board

The Architectural Review Board’s (ARB) purpose is to review the contracted architecture and solutions strategy for the program to verify it aligns to the CUSTOMER NAME REMOVED requirements and expectations in accordance to the SOW and any changes that may be required to the solution. The ARB will be coordinated in alignment to the Program Communication plan. The ARB must include the CUSTOMER NAME REMOVED Program Architect, CUSTOMER NAME REMOVED Domain Architects, and any Microsoft or partner role that has SME input. The ARB is chaired/sponsored by the CUSTOMER NAME REMOVED Program Architect.

The cadence of the ARB meetings will be defined in the Program Communication plan. Each project may choose to host their own solution meetings but all technical solution decisions, changes and strategy that materially impact the Program must be raised in the ARB and documented in the Program team site.

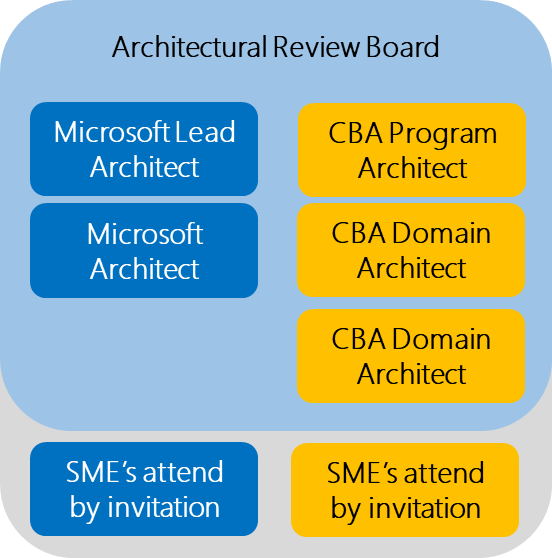


Figure 5: Architectural Review Board

## Program completion

Microsoft will provide Services defined in this SOW to the extent of the term specified in the Work Order. If additional services are required, the Change management process will be followed, and the contract modified.

The program will be considered complete when at least one of the following conditions has been met:

* All Microsoft deliverables that require acceptance have been delivered and accepted (or deemed accepted).
* The Work Order is terminated pursuant to the provisions of the agreement.

If an individual project is terminated, it will be considered complete.

# Program organisation

## Program structure

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

The roles defined below relate to the overall program governance structure, which has unique program leadership roles that do not exist formally in a standard project structure. These roles include: Project Manager and Program Architect.

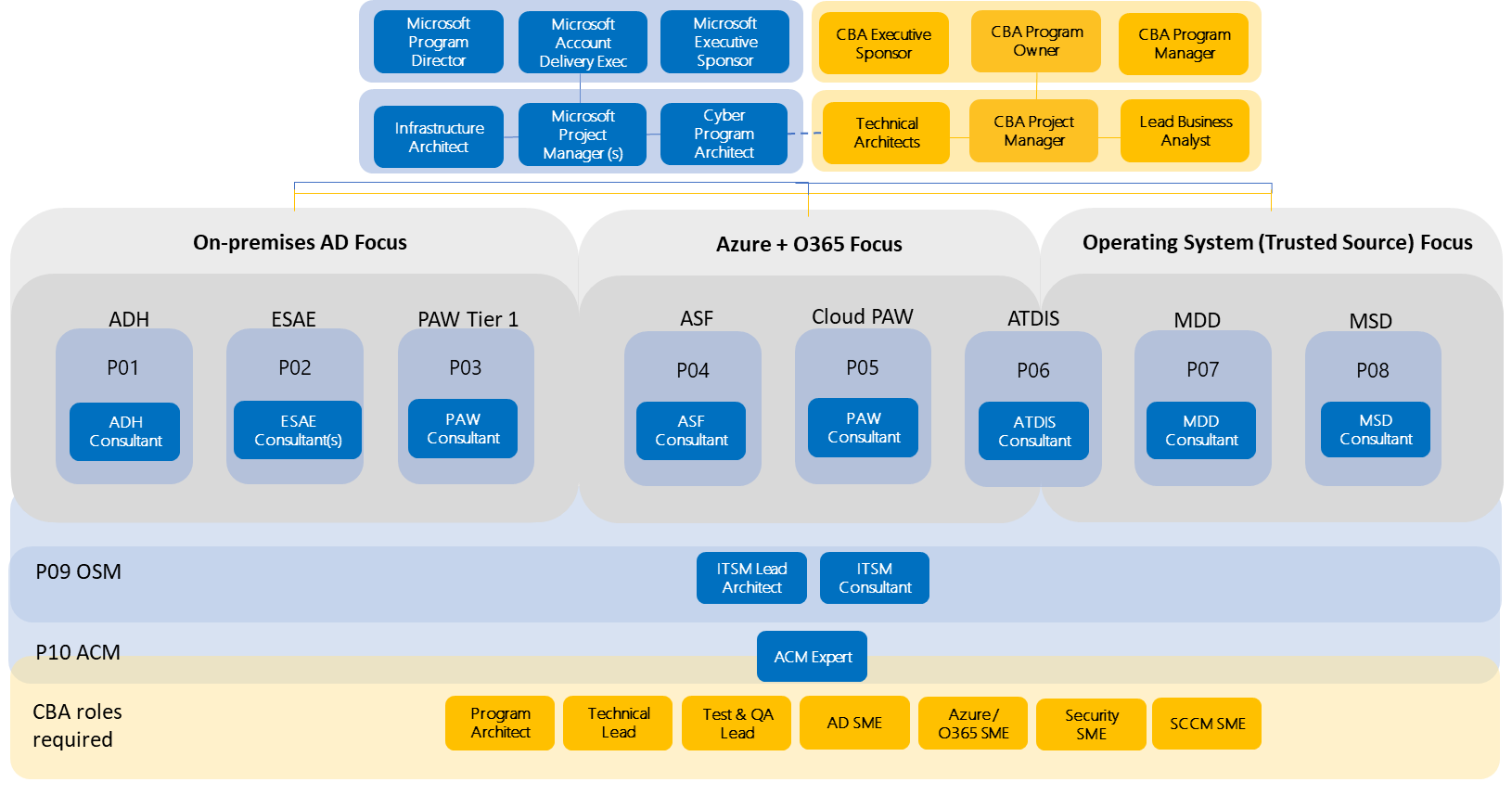


Figure 6: Microsoft & CUSTOMER NAME REMOVED Program Organisation

## Program roles and responsibilities

This section provides a brief description of key program roles and responsibilities with respect to the governance of all projects. For specific roles and responsibilities for individual projects, refer to the relevant project section.

### CUSTOMER NAME REMOVED

The following CUSTOMER NAME REMOVED roles are the consolidated program view and are expected to be working across all of the projects within this program.

Table 11: Program roles and responsibilities - CUSTOMER NAME REMOVED

|  |  |  |
| --- | --- | --- |
| Role | Responsibilities | Estimated Commitment |
| Executive Sponsor | * Arbitrates on all escalations, provide strategic vision, owns Executive Steering Committee decisions. * Align priorities among CUSTOMER NAME REMOVED organisations, early and throughout the program/project. | ¼ day per week |
| Program Owner | * Makes key program decisions, serves as a point of escalation and clears program roadblocks. * Engages leaders and managers, communicates with the organisation, facilitates organisation engagement and participation, builds and maintains support early and throughout the program/project. | 1 day per week |
| Project Manager | * Primary point of contact for Microsoft team. * Responsible for managing and coordinating the overall program and delivering to schedule. * Responsible for CUSTOMER NAME REMOVED resource allocation, risk management, program priorities, and communication to executive management. * Coordinates decisions within three (3) business days, or otherwise agreed timeline. * Manages CUSTOMER NAME REMOVED and/or partner contracts, logistics, collects program data for inclusion into Executive Steering Committee, reviews consolidated risks/issues. | 5 days per week |
| Program Architect | * Responsible for overall architecture decisions for the program for CUSTOMER NAME REMOVED * Represent the program at CUSTOMER NAME REMOVED Internal Architecture Review Boards | 5 days per week |
| Technical Lead | * Serve as primary technical point of contact. * Take ownership of technical architecture and code deliverables. | 5 days per week |
| Test & QA Lead | * Test plans and guides. * Coordinate testing resources for acceptance tests. | 3-5 days per week |
| AD SME | * Technical representation for the CUSTOMER NAME REMOVED Active Directory. | 3-5 days per week |
| Azure & O365 SME | * Provides technical representation for Azure Active Directory and Active Directory Domain Services | 3-5 days per week |
| Security SME | * Technical representation for cybersecurity that relates to the security architecture to be implemented. | 3-5 days per week |
| SCCM SME | * CUSTOMER NAME REMOVED System Centre Configuration Manager technical representative | 5 days per week |
| Process and tooling decision makers | * Decision makers that can enable the modification of current ITSM processes and tooling | 3-5 days per week |
| Process and tooling Subject Matter Experts (SMEs) | * ITSM process SMEs needed to interface with the Microsoft ITSM consultant team * Provide knowledge of existing processes and tooling around support, operations and admin rights delegation | 3-5 days per week |
| ACM: Change Managers | * If the position exists, these managers are the people in the organization normally responsible for implementing change. * Attend activities, sessions, workshops, or classes that are relevant to the change management scope and help drive program change and adoption initiatives. * Be able to commit to 2 days of participation in workshops and meetings. | 3-5 days per week, during the ACM 4-week project (P10) |
| ACM: Business unit leaders | * These managers will implement the transformation of the organization within Business As Usual (BAU) Operations. * Attend activities, sessions, workshops, or classes that are relevant to the business or relevant to the employees in their respective organizations. * Actively support the ACM program. * Participate actively and visibly throughout the project. * Build a coalition of sponsorship with peers and managers. * Communicate effectively with employees and managers. | 1 days per week, during the ACM 4-week project (P10) |
| ACM: Communications Lead | * This member of your organization is responsible for corporate communication, either overall or specifically for technology transformations. * Attend activities, sessions, workshops, or classes relevant to his or her scope of influence and help drive program communication and training initiatives. | 1-3 days per week, during the ACM 4-week project (P10) |
| ACM: Training Lead | * This member of your organization is responsible for technology training. * Attend activities, sessions, workshops, or classes relevant to his or her scope of influence and help drive program communication and training initiatives. | 1-3 days per week, during the ACM 4-week project (P10) |
| ACM: Human resources (HR) Lead | * This member of your organization’s HR group will be empowered to assist with the program from a personnel perspective and can provide input on the potential effects of the technology change such as organizational effects, fears of job loss, or swings in morale. * Determine any potential effects to company HR policies brought on by the change program and promote mitigation of any such HR conflicts. | 1-3 days per week, during the ACM 4-week project (P10) |
| ACM: Change agents | * These are specific members within your organization who can positively guide members of the target audiences toward making necessary changes. | 1-3 days per week, during the ACM 4-week project (P10) |
| ACM: Change community leaders | * These leaders, who are selected from the change agents, are usually 1 or 2 individuals who act as leaders and manage the overall community. | 1-3 days per week, during the ACM 4-week project (P10) |

### Microsoft

Table 12: Program roles and responsibilities - Microsoft

|  |  |
| --- | --- |
| Role | Responsibilities |
| Account Delivery Executive | * Serve as a single point of contact for escalations, billing issues, personnel matters and contract extensions. * Act as primary contact for Executive Stakeholders. * Accountable for Microsoft’s capability to deliver and achieve against written objectives. * Participate in Project Governance activities as appropriate. * Work with the Program sponsors to resolve issues that could not be resolved by the Project manager. * Prepare Executive Steering Committee materials and chair monthly Steering Committee Meetings. |
| Program Director | * Consolidate all Project status, risks, issues, deliverables and escalations. * Prepare Program and Executive Steering Committee materials. * Analyse Program interfaces and Program critical dependencies between all work and recommend appropriate actions to the relevant governance forums * Provide rigorous change control, registering changes for impact analysis and resolution. * Validate that items requiring action be resolved in a timely fashion, reporting status and escalation as required. * Commission and chair reviews both during the (Microsoft) Program and following Program closure that formally assess the Program’s continued alignment with CUSTOMER NAME REMOVED’s objectives, Microsoft’s capability to deliver and achievement against objectives. * Plan and design the Program and proactively monitor its overall progress, resolve issues and initiate corrective action as appropriate through the Program Steering Committee or Leadership roles. * Initiate extra activities and other management interventions wherever gaps in the Microsoft Program are identified or issues arise. * Report progress of the Microsoft Program at regular intervals per Program Governance and Communications plan. * Establish and implement the Program management processes through Program forums. * Verify delivery of all deliverables as per the Program Master Schedule |
| Project Manager | * Fully accountable for communicating to the Program Leadership. * Plan and design the projects and proactively monitor its overall progress, resolve issues and initiate corrective action as appropriate through the Executive Steering Committee or Leadership roles. * Accountable for Microsoft’s capability to deliver and achieve against written objectives. * Participate in Executive Steering Committee as appropriate. * Review and approve user access and standards of all internal supporting tools (i.e., Project Server & TFS). * Schedule and host monthly internal Microsoft Program Quality Review Boards (PRB, PMR) with Microsoft leadership. * Consolidate all project status, risks, issues, deliverables and escalations. * Provide rigorous change control, registering changes for impact analysis and resolution. * Validate that items requiring action are resolved in a timely fashion, reporting status and escalation as required. * Initiate extra activities and other management interventions wherever gaps in the Microsoft program are identified or issues arise. * Accountable for all Program Financials Reporting. * Define and partner with Program Management roles on program charter and communication plan. |
| Cyber Program Architect | * Coordinates solution design across all projects. * Review architecture designs to facilitate compliance with program and architectural guidelines. * Participates in architectural envisioning workshops as requested. * Act as the Program’s Centralised Design Authority. * Lead and contribute to Architect Review Board (ARB). * Provide solution and technical consulting and guidance to CUSTOMER NAME REMOVED as applicable. * Review and guide the team solution strategy, dependencies and technical innovation. * Participate and contribute to all Product team discussions that materially impact or cause risk to the program. * Own and document technical traceability to the SOW for delivery and report status to Microsoft Project Manager * Review all major deliverables for technical soundness and quality. * Define and Manage Technical disciplines such as code reviews, code check in, documentations at the program level as needed. * Act and provide technical leadership escalation path for all program architect strategy. * Review and define technical partner quality KPIs with ARB members and report status to Microsoft Project Manager |
| Infrastructure Architect | * Provides architectural leadership for Microsoft Infrastructure components of the solution so that recommended methodologies are followed, * Reviews all engagement deliverables and identifies and manages risk. |

# CUSTOMER NAME REMOVED responsibilities and program assumptions

## CUSTOMER NAME REMOVED responsibilities

In addition to CUSTOMER NAME REMOVED activities defined in the Approach section, CUSTOMER NAME REMOVED is also required to:

* **Provide information**
  + This includes accurate, timely (within 3 (three)) business days or as mutually agreed-upon), and complete information.
* **Provide access to people and resources** 
  + This includes access to knowledgeable CUSTOMER NAME REMOVED personnel, including business user representatives, and access to funding if additional budget is needed to deliver project scope.
  + CUSTOMER NAME REMOVED is responsible for obtaining all required licenses and products.
* **Provide access to systems**
  + This includes access to all necessary CUSTOMER NAME REMOVED work locations, networks, systems, and applications (remote and onsite).
* **Provide a work environment**
  + This consists of suitable workspaces, including desks, chairs, and Internet access.
* **Manage non-Microsoft resources**
  + CUSTOMER NAME REMOVED will assume responsibility for the management of all CUSTOMER NAME REMOVED personnel and vendors who are not managed by Microsoft.
* **Manage external dependencies**
  + CUSTOMER NAME REMOVED will facilitate any interactions with related projects or programs in order to manage external project dependencies.

## Program assumptions

The program scope, services, fees, timeline, and our detailed solution are based on the information provided by CUSTOMER NAME REMOVED to date. During the program, the information and assumptions in this SOW will be validated, and if a material difference is present, this could result in Microsoft initiating a change request to cover additional work or extend the program duration. In addition, the following assumptions have been made:

* **Workday** 
  + The standard workday for the Microsoft team is between 8 AM and 5 PM, Monday through Friday.
* **Standard holidays**
  + Observance of consultants’ country-of-residence holidays is assumed and has been factored into the project timelines.
* **Remote working**
  + The Microsoft team may perform services remotely.
  + If the Microsoft team is required to be present at the CUSTOMER NAME REMOVED location on a weekly basis, resources will typically be on site for 3 (three) nights and 4 (four) days, arriving on a Monday and leaving on a Thursday.
* **Language**
  + All communications and documentation will be in English. Local language support and translations will be provided by CUSTOMER NAME REMOVED.
* **Staffing**
  + If necessary, Microsoft will make staffing changes. These can include, but are not limited to, the number of resources, individuals, and project roles.
  + Microsoft Project team members include non-Australian citizens and members of the Microsoft Global Delivery team from India.
  + Microsoft will use subcontractors to perform services under this Program, Microsoft will be responsible for their performance subject to the terms of this agreement.
* **Informal knowledge transfer**
  + CUSTOMER NAME REMOVED staff members who work alongside Microsoft staff will be provided with informal knowledge transfer throughout the program. No formal training materials will be developed or delivered as part of this informal knowledge transfer. Informal knowledge transfer is defined as informal information that is shared when CUSTOMER NAME REMOVED staff works side by side with Microsoft staff. This could include whiteboard discussions, email threads, conference calls, and facilitated meetings regarding technical topics.
* **Mobilisation**
  + The project start date will be mutually agreed by Microsoft and CUSTOMER NAME REMOVED after the associated work order is fully executed and is subject to resource availability and visa processing times.
  + Typical mobilisation is 6 (six) weeks, depending on visa requirements visa processing durations. If the mobilisation period is shorter, and subject to resource availability, the start date may be brought forward by mutual agreement. Likewise, if the visa processing is longer in duration than six weeks, the mobilisation period may be extended.

# P01: Active Directory Hardening (ADH)

The scope of this project is to assist CUSTOMER NAME REMOVED with discovering existing privileged access within their production Active Directory Domain Services (AD DS) environment which will be documented within an exposure report document. This information will provide context for establishing a transition plan so CUSTOMER NAME REMOVED may transition into Microsoft’s recommended model for administering Active Directory. This is referred to as “Microsoft’s Reference Architecture for Active Directory Administration”.

Microsoft’s Reference Architecture for Active Directory Administration focuses on a tiered model for Active Directory administration. The tiered model for Active Directory administration is as follows:

* **Tier 0** – In an enterprise environment, Tier 0 includes all administrators in control of the Active Directory forest, domains, and domain controllers and systems which operate or manage Tier 0 resources (i.e. monitoring & A/V). In this project, we will focus on the administrative user objects contained within the following Active Directory groups which have the most control over Tier 0 resources; Enterprise Admins, Domain Admins, Schema Admin, BUILTIN\Administrators, Account Operators, Backup Operators, Print Operators, Server Operators, Group Policy Creators Owners, and Cryptographic Operators.
* **Tier 1** – In an enterprise environment, Tier 1 includes all administrators who are in control of multiple server operating systems, enterprise application administrators, and administrators of cloud services. These are not in scope for this project.
* **Tier 2** – In an enterprise environment, Tier 2 includes administrative roles that have administrative rights to provide user, computer, and device support. These are not in scope for this project.

Given that Tier 0 focuses on credentials that when compromised may provide an attacker highly privileged access to any resource secured by Active Directory, our focus will be to assist CUSTOMER NAME REMOVED with moving into the recommended model for Active Directory Administration.

## Objectives

The objective of this project is to support CUSTOMER NAME REMOVED to improve the security posture of their production Active Directory administrative environments by:

* Discover, analyse and share CUSTOMER NAME REMOVED’s existing security exposure for high-value Active Directory assets.
* Assess and analyse privileged account exposure and provide a migration plan for deviations from Microsoft security recommendations.
* Facilitate, plan and prepare CUSTOMER NAME REMOVED for deploying a recommended Active Directory administration model.
* Deploy the Microsoft Security Administration model to the target Active Directory domains in scope.
* Active Directory Hardening utilises enhanced technologies and recommended practices to provide enhanced security protection and security controls to:
  + Tier 0 (highly privileged top-level accounts);
  + Tier 1 (server workload privileged accounts); and
  + Tier 2 (privileged accounts for support desk operations).
* Providing training workshops to share Microsoft recommended practices for administering high-value Active Directory assets.
* Assist CUSTOMER NAME REMOVED with reducing the number of highly privileged Active Directory administrative accounts by implementing, and moving into, a recommended Active Directory administration model.
* Provide support and guidance to the AD consolidation teams with a focus on technical requirements, supported configuration patterns, operational risks and guidance on migration practices and processes to consolidate Active Directory domains

## Areas in scope

### General project scope

To deliver the Active Directory Hardening solution for CUSTOMER NAME REMOVED, Microsoft will provide the following services:

Table 13: ADH – General project scope

|  |  |  |
| --- | --- | --- |
| Area | Description | Assumptions |
| Tier 0 exposure analysis | * Discover and analyse Tier 0 privileged credentials within up to ten (10) Active Directory Domain Services (AD DS) domains. * Discover and analyse privileged credential exposure on member servers located within the in-scope AD DS domain. Specifically:   + - Service accounts running with elevated privileges.     - Elevated privileges within the - local administrator group. | * CUSTOMER NAME REMOVED completes all appropriate change management processes to deploy the data collection component of the analysis tools. * CUSTOMER NAME REMOVED deploys the data collection component of the analysis tools to all appropriate systems (domain controllers and servers) within the environment required to meet the scope of this engagement. * A minimum of .NET Framework 4.5.2 or above is present on the target servers for data collection prior to the start of the workstream |
| Tier 0 transition planning workshops | * Conduct up to eleven (11) transition planning workshops per each in scope domain focused on: * Group policy settings review and planning [Default domain and default domain controllers’ group policy objects (GPOs); up to two (2) hours. * Transitioning enterprise admins, domain admins and administrators to recommended AD DS admin model groups; up to eight (8) hours. * Transitioning group policy creator owners’ group to recommended AD DS admin model groups; up to two (2) hours. * Transitioning server operators to recommended AD DS admin model groups; up to two (2) hours. * Transitioning account operators to recommended AD DS admin model groups; up to one (1) hour. * Transitioning backup operators to recommended AD DS admin model groups; up to one (1) hour. * Transitioning cryptographic operators to recommended AD DS admin model groups; up to one (1) hour. * Transitioning virtualisation admins to recommended AD DS admin model groups; up to one (1) hour. * Splitting accounts that currently have privileges to multiple tiers; up to four (4) hours. * Plan for implementing a group of critical machines that will be used by Tier 0 users; up to two (2) hours. * Plan for blocking Tier 0 users from navigating to the Internet (proxy block); up to two (2) hours. | * The Tier 0 Transition Plan document contains the results of the Tier 0 transition planning workshops. * Transition planning workshops are domain dependant and often sperate team dependant; Microsoft will look to combine relevant workshops as agreed at the start of the engagement. * This document will be used to move users into their new Active Directory administrative group once the recommended Tier 0 configuration is deployed. |
| Implement recommended and preconfigured AD DS administrative model | * Deploy recommended AD DS administration model to up to ten (10) production AD DS domains including:   + - Organisation unit (OU) structure including a new Computer Quarantine OU.     - GPOs with baseline security recommendations.     - Administrative groups and associated AD DS delegations. * Link and activate new default domain, default domain controllers, and computer quarantine GPOs. * Transition and validate AD DS user objects out of default administrative groups into appropriate new tiered model group; up to thirty (30) hours per in scope domain. * Provide post-deployment operational assistance for up to sixteen (16) hours per in scope domain. | * Microsoft will support CUSTOMER NAME REMOVED during the process of implementing the recommended and preconfigured AD DS administrative model into the production AD DS environment. |
| AD Consolidation Guidance and Support | * AD Conslidation - Assessment guidance timeboxed to twelve (12) weeks. * AD Conslidation - Planning guidance timeboxed to twelve (12) weeks | * CUSTOMER NAME REMOVED is responsible for providing the domains that are in scope for the assessment * AD consolidation activities will be performed by CUSTOMER NAME REMOVED |

### Environments

The following environments will be required to deliver the project.

Table 14: ADH – Environments

|  |  |  |  |
| --- | --- | --- | --- |
| Environment | Location | Responsibility | Ready by |
| Production Active Directory domain | CUSTOMER NAME REMOVED | CUSTOMER NAME REMOVED | Start of engagement |

### Testing

The following testing is included in the scope of the project. If CUSTOMER NAME REMOVED has responsibility for testing, the Microsoft effort to support that activity is identified. If additional time is needed for Microsoft testing support, then it can be requested through the Change management process described in this SOW.

Table 15: ADH – Testing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test type (environment) | Description | Responsibility | | |
| Has responsibility for testing? | Provides data or test cases | Provides guidance and support |
| System testing (Test) | System testing focuses on system functionality meeting the design. Test cases are based on the Test Plan document and include functionality tests of the new Tier 0 administrative model and the validation of the preconfigured permissions against the new structure. The Microsoft effort to support this testing is limited to eight (8) hours per domain in scope. | CUSTOMER NAME REMOVED | Microsoft | Microsoft |

### Training

The following Instructor-led training will be delivered during this project.

Table 16: ADH – Training

|  |  |  |
| --- | --- | --- |
| Location | Description | Quantity and duration |
| CUSTOMER NAME REMOVED Sydney | * Microsoft Secure Modern Enterprise Foundations * Materials**:** PowerPoint presentation * Project phase:Envision | * Number of sessions: 1 Duration: 1 hour * Number of participants: up to 30 |
| * Understanding Credential Theft * Materials: PowerPoint presentation * Project phase: Envision | * Number of sessions: 1 * Duration: 2 hours * Number of participants: up to 30 |
| * Overview of Microsoft’s Tiered Administration Model * Materials: PowerPoint presentation * Project phase: Envision | * Number of sessions: 1 Duration: 2 hours * Number of participants: up to 30 |
| * Overview of the Tier 0 Configuration Model – Administration and Delegation Model Overview * Materials: PowerPoint presentation * Project phase: Envision | * Number of sessions: 1 Duration: 4 hours * Number of participants: up to 30 |
| * Overview of the Design and Implement Active Directory Configuration Model – Secure Group Policies Overview * Materials: PowerPoint presentation * Project phase: Envision | * Number of sessions: 1 Duration: 2 hours * Number of participants: up to 30 |
| * Active Directory Hardening Discovery Tools Overview Workshop * Materials: PowerPoint presentation * Project phase: Envision | * Number of sessions: 1 Duration: 2 hours * Number of participants: up to 30 |

## Areas out of scope

Any area not explicitly included in the Areas in scope section is out of scope for Microsoft during this project. Areas out of scope for this project, in addition to those listed elsewhere in this document, are listed in the following table.

Table 17: ADH – Out of scope

|  |  |  |
| --- | --- | --- |
| Area | Description | |
| Role definition | Custom definition of roles and the creation of new accounts or roles (such as groups) are out of scope. This project will utilise a predetermined administrative model as provided by the recommended AD DS administration model. |
| AD Consolidation | Any activities related to AD consolidation |

## Approach

The project will be structured following the Microsoft solution delivery methodology across five distinct phases: Envision, Plan, Build, Stabilise, and Deploy. Each phase has distinct activities that are described in the following sections.

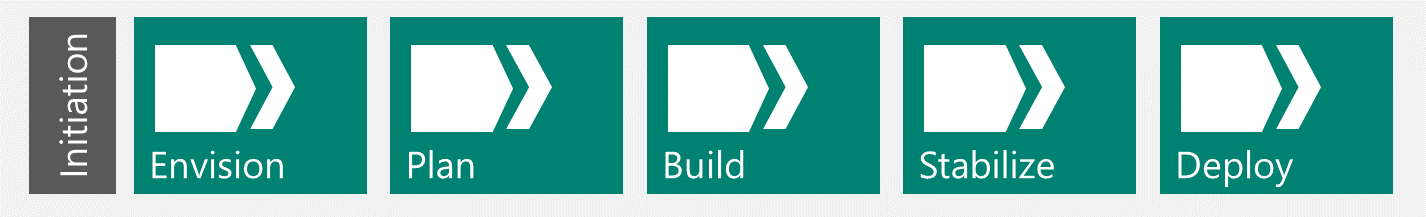


Figure 7: ADH – Approach

### Envision

During the Envision phase, the team will identify and define the requirements for the overall solution, gain an understanding of the environment, design a high-level solution strategy that meets the requirements of the solution, define the roles and responsibilities of the project team, and create a Vision and Scope document identifying what will be accomplished.

Additionally, Microsoft will provide CUSTOMER NAME REMOVED with a series of training workshops to help prepare CUSTOMER NAME REMOVED for reviewing the Tier 0 Exposure Report, planning administrative user transitions, and completing Tier 0 administrative user object movement into the recommended Tier 0 configuration model.

Table 18: ADH – Envision activities

|  |  |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | * Conduct kick-off and scope validation meeting. * Lead one (1) requirements gathering workshop lasting no more than one (1) hour in total for each domain. * Develop vision and scope document. * Conduct training as defined in the Training section 5.2.4. |
| **CUSTOMER NAME REMOVED activities** The activities to be performed by CUSTOMER NAME REMOVED | * Participate in project kick-off meeting and workshops. * Participate in requirement gathering workshops. * Participate in the AD consolidation assessment workshops * Provide requested information and documentation. * Review, accept and approve the vision and scope document. * Identify appropriate personnel to attend training workshops. * Attend training workshops. |

### Plan

During the Plan phase, Microsoft will work with CUSTOMER NAME REMOVED to use the analysis tools to begin gathering information about Tier 0 resources. Using this information, Microsoft will lead and conduct sessions to review data that has been collected with CUSTOMER NAME REMOVED and will produce a Tier 0 Exposure Report highlighting areas CUSTOMER NAME REMOVED should consider further investigating.

The activities within this phase are to prepare CUSTOMER NAME REMOVED for the deployment of the new Tier 0 administration model and the transition of existing administrative accounts into this model.

Table 19: ADH – Plan activities

|  |  |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | * Assist with ADH tools deployment; up to 12 hours per domain. * Assist with the remediation of data collection issues; up to four (4) hours per domain. * Process collected data. * Perform Tier 0 analysis and information preparation. * Create the Tier 0 exposure report, one (1) per domain. * Conduct Tier 0 exposure review meeting with CUSTOMER NAME REMOVED. * Conduct Tier 0 transition planning workshops with CUSTOMER NAME REMOVED. * Document Tier 0 Transition Plan, one (1) per domain. * Conduct Tier 0 Transition Plan review meeting with CUSTOMER NAME REMOVED. * Participate in the AD consolidation planning workshops |
| **CUSTOMER NAME REMOVED activities** The activities to be performed by CUSTOMER NAME REMOVED | * Provide requested information and documentation. * Participate in Tier 0 transition planning workshops. * Review the Tier 0 Exposure Report. * Review, accept, and approve the Tier 0 Transition Plan document. |

### Build

The Build phase focuses on the deployment of the recommended AD DS administration model into CUSTOMER NAME REMOVED’s production AD DS using automation scripts provided by Microsoft. This includes the deployment of:

* **GPOs:** The deployment of the new GPOs does not include linking the GPOs to an OU. This process will occur during the Deploy phase.
* **Tier 0 OUs:** these will be newly created OUs that will be placed into CUSTOMER NAME REMOVED’s production Active Directory environment. Movement of objects into the new OU structure will occur during the Deploy phase.
* **Tier 0 administrative groups:** the deployment of the recommended Tier 0 administrative groups. The movement of users into these groups will follow information documented in the Tier 0 Transition Plan and will occur during the Deploy phase.
* **Tier 0 administrative delegations:** using the new Tier 0 administrative groups and OUs, delegations will be completed by applying recommended permissions to both the Tier 0 administrative groups and the appropriate Tier 0 OU.

While this configuration will be deployed during this phase, activation of the configuration does not occur until the Deploy phase after CUSTOMER NAME REMOVED, with the assistance of Microsoft, tests and validates the configuration during the Stabilise phase.

Table 20: ADH – Build activities

|  |  |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | Assist CUSTOMER NAME REMOVED in implementing the recommended AD DS administration model into production AD DS domains. |
| **CUSTOMER NAME REMOVED activities** The activities to be performed by CUSTOMER NAME REMOVED | Implement the recommended AD DS administration model into the production AD DS environments. |

### Stabilise

During the Stabilise phase, testing of the recommended Tier 0 configuration will be completed. The intention of this phase is to test and validate that the recommended Tier 0 configuration functions as designed, and that test users, who have been granted access in the new Tier 0 configuration, have appropriate permissions as designed.

Table 21: ADH – Stabilise activities

|  |  |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | * Assist with system testing. * Create Test Plan document with testing results. * Lead a meeting to review test results with CUSTOMER NAME REMOVED. |
| **CUSTOMER NAME REMOVED activities** The activities to be performed by CUSTOMER NAME REMOVED | * Perform system testing. * Attend the test results review meeting. * Review, accept, and approve the Test Plan document. |

### Deploy

The Deploy phase consists of transitioning existing privileged accounts to the new Tier 0 configuration. The transition of existing resources to the new Tier 0 configuration consists of the following:

* Activation and linking of GPOs to the domain and domain controllers’ OUs
* Moving users out of the default AD DS administrative groups into the appropriate group within the new recommended AD DS administrative model following the Tier 0 Transition Plan document.

Table 22: ADH – Deploy activities

|  |  |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | * Link and activate new default domain, default domain controllers, and computer quarantine GPOs. * Transition and validate AD DS user objects out of default administrative groups into appropriate new tiered model group. * Provide operational assistance as defined by the scope of this project. * Conduct project closeout. |
| **CUSTOMER NAME REMOVED activities** The activities to be performed by CUSTOMER NAME REMOVED | * Link and activate new default domain, default domain controllers, and computer quarantine GPOs. * Transition and validate AD DS user objects out of default administrative groups into appropriate new tiered model group. * Participate in project closeout. |

## Deliverables

This section provides a list of the deliverables produced by the ADH project. If a deliverable requires formal review and acceptance (indicated by a Yes), it will be governed by the deliverable acceptance process as defined in section 2.5.

Table 23: ADH – Deliverables

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Phase | Deliverable name | Deliverable Description | Acceptance Required | Responsibility |
| D06 | Envision | ADH Vision and Scope document | Microsoft Word document that unifies the team on the target solution and overall project direction. | Yes  Acceptance Criteria:  A Microsoft Word document of approximately 20 to 50 pages, that contains the information agreed during the Envisioning workshop. | Microsoft |
| D07 | Plan | Tier 0 Exposure Report | A Microsoft Excel file which contains information collected using the ADH tools during the Discovery and Analysis phase. | No | Microsoft |
| D08 | Plan | Tier 0 Transition Plan | Word document describing the results of the Tier 0 transition planning workshops. This document will be used to move users into their new Active Directory administrative group once the recommended Tier 0 configuration is deployed.  One (1) document per Domain | Yes  Acceptance Criteria:  A Microsoft Word document contains complete and accurate information about Service accounts running with elevated privileges discovered using the ADH tools. | Microsoft |
| D09 | Stabilise | Test Plan document | A Word document that includes test results and notes about implementing the defined test cases.  One (1) document per Domain | Yes  Acceptance Criteria:  A Microsoft Word document of approximately 25 – 40 pages, that includes the expected test results and notes about implementing the defined test cases. | Microsoft |

## Project roles and responsibilities

The key project roles and the responsibilities are as follows:

### CUSTOMER NAME REMOVED

Required CUSTOMER NAME REMOVED Roles are defined at the Program level in section 3.2.1.

### Microsoft

Table 24: ADH – Microsoft roles and responsibilities

|  |  |
| --- | --- |
| Role | Responsibilities |
| ADH Consultant | * Full time. * Provide technical oversight. * Verify whether Microsoft-recommended practices are followed. * Responsible for project outcome and solution design and deployment. * Facilitate workshops outlined in section 5.2.4 and 5.4. |

## CUSTOMER NAME REMOVED responsibilities and project assumptions

### CUSTOMER NAME REMOVED responsibilities

In addition to CUSTOMER NAME REMOVED activities defined elsewhere in this document, CUSTOMER NAME REMOVED is also required to:

* Deploy the data collection component of the analysis tools to all appropriate systems (Domain Controllers and Servers) within their environment required to meet the scope of this engagement.
* Move the users from their current group memberships into the destination group as defined by the Transition Plan workshop and documented within the Transition Plan document.

### Project assumptions

The project scope, services, fees, timeline, and our detailed solution are based on the information provided by CUSTOMER NAME REMOVED to date. During the project, the information and assumptions in this document will be validated, and if a material difference is present, this could result in Microsoft initiating a change request to cover additional work or extend the project duration. In addition to the assumptions elsewhere in this document, the following assumptions have been made:

* Managed Servers are Active Directory domain joined.
* Only Windows Server operating systems in main or extended lifecycle support are in scope (Windows Server 2008 and above). Windows Server operating systems or versions under custom agreements will not be supported.
* Microsoft assumes that all machines have the default admin shares turned on.
* A minimum of .NET Framework 4.5.2 or higher is installed on the target systems prior to engagement start
* Data collection is limited to systems that can be reached by collection tools. Network segmentation may result in suboptimal coverage of data collection.

# P02: Enhanced Security Administrative Environment (ESAE)

## Objectives

The objective of this project is to implement the Enhanced Security Administrative Environment (ESAE) for up to ten (10) domains).

ESAE provides advanced protections for Tier-0 highly privileged top-level accounts (Domain Administrators, Enterprise Administrators, and equivalent) based upon Microsoft’s recommended practices, architectures, and accumulated field experience.

ESAE helps protect these Tier-0 accounts with dedicated administrative workstations, enhanced hardened security controls and configurations, and a dedicated environment to administer identity within the organisation.

CUSTOMER NAME REMOVED has identified ten (10) Active Directory domains of critical importance and has indicated that a consolidation is complex and not in the short-term plan. Therefore, in order to support the protection of these critical accounts the Enhanced Security Administrative Environment (ESAE) will be used to protect ten (10) domains and take control of these privileged accounts.

## Areas in scope

### General project scope

Microsoft will provide Services in support of the following scope.

Table 25: ESAE - General project scope

|  |  |  |
| --- | --- | --- |
| Area | Description | Assumptions |
| Envisioning workshops | Conduct envisioning workshops that cover:   * Project kick-off: introduce the project team, objectives, delivery framework, and so on. * Solution Envisioning: discuss current state, requirements, and end state objectives. | Up to six (6) workshops, 4 hours per domain in scope. |
| Design workshops | Conduct design workshops that cover the functional definitions for in-scope ESAE features for up to ten (10) domains | Up to six (6) workshops, 4 hours per domain in scope. |
| ESAE design | Configure the ESAE reference architecture to fit CUSTOMER NAME REMOVED environment. | * ESAE reference architecture and product set will be used. * Environment contains up to forty (40) production domain controllers. |
| ESAE Administrative Workstation image | Implement one (1) Administrative Workstation image per domain. | One (1) device model will be used for Administrative Workstations. |
| Network traffic security | Design and configure IP security (IPsec) and purpose-build Public Key Infrastructure (PKI) Certification Authority (CA) in ESAE environment. |  |
| Smart card configuration | Design, configure, and deploy up to ten (10) CUSTOMER NAME REMOVED supplied smart cards to administrators. | * One (1) type of smart card will be used. * Smart cards are compatible with the Microsoft Base Smart Card Cryptographic Service Provider standard. * Distribution will not require travel. |
| Security alerting | Plan and configure security alerting for ESAE and production domain controllers using System Center Operations Manager and management agents. | No custom tuning of supplied health monitoring is required. |
| Build and connect ESAE to Production environment | * Build and configure one (1) ESAE environment. * Configure up to four (4) Domain controllers, located on up to two (2) different network segments (subnets), for the ESAE environment. * Connect ESAE to ten (10) production domains. * Support CUSTOMER NAME REMOVED configuration of up to thirty-six (36) additional Domain controllers for the ESAE environment. | One (1) production instance of ESAE will be deployed; the instance created and tested in the Build environment will be moved to the datacentre and connected to the production environments. |
| Operations Guide | Document the recommended operational guidance and practices for using and maintaining the security infrastructure and systems within the ESAE. | CUSTOMER NAME REMOVED or a CUSTOMER NAME REMOVED service partner will run and maintain the ESAE infrastructure. |
| Use Hardware Security Module (HSM) | Integrate ESAE CA with an HSM. | * HSM is compatible with Active Directory Certificate Services. * The HSM is only used to store the CA private key. Any other use of HSM may require additional offerings such as the “PKI Implementation Services” offering. |
| Integrate with Security Information and Event Management (SIEM) | Establish a data connection and define filters so that events from ESAE can be collected in a central SIEM solution. | Deploy log analytics or CUSTOMER NAME REMOVED supplied SIEM solution. |
| Integrate with existing backup | Deploy a backup agent, test ESAE configuration, and assess the security posture. | - |
| Implement Hyper-V high availability | Design and implement a Hyper-V high-availability solution. | - |

### Software products and technologies

The products and technology that are listed in the following table are required for project implementation. CUSTOMER NAME REMOVED is responsible for obtaining all identified licenses and products.

Table 26: ESAE - Software products and technologies

|  |  |  |
| --- | --- | --- |
| Product and technology item | Version | Ready by |
| Windows Server | 2016 | Prior to Plan phase |
| Windows | 10 Enterprise x64 | Prior to Plan phase |
| Microsoft SQL Server | Standard 2016 | Prior to Plan phase |
| System Center Operations Manager | 2016 | Prior to Plan phase |

Additional Microsoft 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 these required files.

### Environments

The following system environments describe the development and test facilities to be used by the project team members. For the following environments, CUSTOMER NAME REMOVED is 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 CUSTOMER NAME REMOVED team will install and configure the software products as described in Software products and technologies section of this document.

The ESAE will be developed in a dedicated security-enhanced room (Test environment) before being connected to the Production environment. The security-enhanced room should meet the following criteria:

* Provide security-enhanced physical access to project materials and all hardware prior to deployment.
* Provide conference facilities with desks and chairs for workshops, meetings, and interviews.
* Provide network connections that give the Microsoft onsite team access to the Internet and email.
* Provide a separate dedicated Internet connection with at least 4 Mbps downstream to be used for the Known Good Media build process.
* Provide a security-enhanced place for storage of all documentation and DVDs used for the project.
* Provide at least one DVD writer device (external or built-in).
* Provide a stack of 20 writable DVDs (single layer).
* Provide a high-speed printer.
* Provide at least five unused and unopened laptops or desktops.
* Provide air-conditioning appropriate for the room and all the equipment in the room.
* Provide a projector.

Table 27: ESAE - System environments

|  |  |  |  |
| --- | --- | --- | --- |
| Environment | Location | Responsibility | Ready by |
| Test (dedicated security-enhanced room) | CUSTOMER NAME REMOVED | CUSTOMER NAME REMOVED | One week prior to the start of Build phase |
| Production | CUSTOMER NAME REMOVED | CUSTOMER NAME REMOVED | One week prior to the start of Deploy phase |

### Testing

CUSTOMER NAME REMOVED has responsibility for testing, the Microsoft effort to support that activity is identified. If additional time is needed for Microsoft testing support, then it can be requested through the Change management process described in this SOW.

Table 28: ESAE - Testing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test type (environment) | Description | Responsibility | | |
| Has responsibility  for testing? | Provides data or test cases | Provides guidance and support |
| System testing  (Test) | System testing focuses on the functionality of achieving expected results. Test cases are based on the test guide document.  The Microsoft effort to support this testing is limited sixty-four (64) hours. | CUSTOMER NAME REMOVED | Microsoft and CUSTOMER NAME REMOVED | Microsoft |
| UAT  (Production) | The user functionality of key real-world (administrator) scenarios will be tested. Test cases are based on the Operations Guide document.  The Microsoft effort to support this testing is limited to twenty-four (24) hours. | CUSTOMER NAME REMOVED | CUSTOMER NAME REMOVED | Microsoft |

## Areas out of scope

Any area not explicitly included in the Areas in scope section is out of scope for Microsoft during this project. Areas out of scope for this project, in addition to those listed elsewhere in this document, are listed in the following table.

Table 29: ESAE - Out of scope

|  |  |  |
| --- | --- | --- |
| Area | Description | |
| General production domain hardening | ESAE helps secure only Tier 0 user accounts; it does not help secure other components of Active Directory Domain Services (AD DS). General hardening of servers such as Domain controllers is out of scope. |
| Improving the security on any Services other than Domain controllers and associated forest or domain-level administration accounts | This project looks only at securing Tier 0 of the Active Directory infrastructure. Providing a security-enhanced administration environment for standard user workstations or laptops and for applications servers (such as Microsoft Exchange, Microsoft SharePoint, or SQL Server) is out of scope. |
| Older operating systems | Support for admin desktops that use an operating system version or image configuration other than those included in the project scope is out of scope. |
| Remote access and administration of Tier 0 | Microsoft does not recommend the use of remote administration for Tier 0 Services. Direct network access to the ESAE forest is recommended. |
| Disaster recovery | Setup and configuration of disaster recovery sites at multiple datacentres is out of scope. Fault tolerance and clustering for high availability or disaster recovery is out of scope. |

## Approach

The project will be structured following the Microsoft Solution Delivery Methodology across five distinct phases: Envision, Plan, Build, Stabilise, and Deploy. Each phase has distinct activities that are described in the following sections.

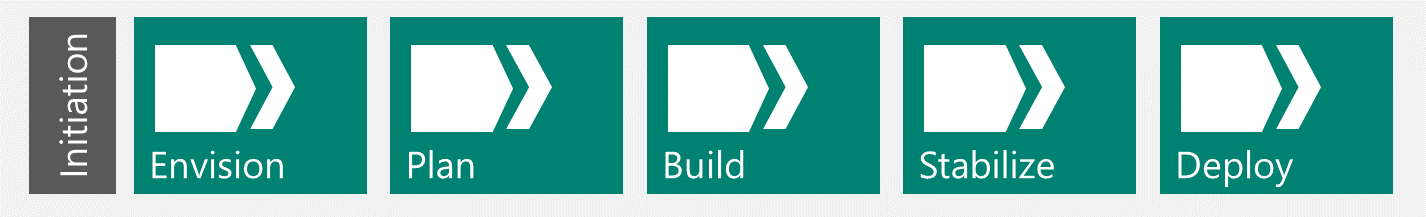


Figure 8: ESAE - Approach

### Envision

During the Envision phase, the team develops the project vision and scope that aligns expectations between the project team and stakeholders. The Envision phase ends when the Vision and Scope document is approved. This milestone indicates that the team is aligned to a common vision and the specific scope of work necessary to bring the vision to reality.

Table 30 - ESAE - Envision phase

|  |  |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | * Conduct kick-off and scope validation meetings. * Conduct envisioning workshops. * Create Vision and Scope document and review with CUSTOMER NAME REMOVED |
| **CUSTOMER NAME REMOVED** **activities** The activities to be performed by CUSTOMER NAME REMOVED | * Identify key stakeholders and help make sure they attend relevant meetings and workshops. * Facilitate communication and requests for information from the Microsoft team. * Make decisions when options are presented. * Review and approve documentation produced by Microsoft as required. |

### Plan

During the Plan phase, the team prepares the Architecture and Design document, works through the design, and prepares detailed work plans documenting what is to be delivered and when.

Table 31: ESAE - Plan phase

|  |  |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | * Conduct design workshops for each of the ten (10) domains. * Create the Architecture and Design document reflecting each of the ten (10) domains and review with CUSTOMER NAME REMOVED . * Update program plan to reflect a detailed timeline for Build, Stabilise, and Deploy phases. |
| **CUSTOMER NAME REMOVED** **activities** The activities to be performed by CUSTOMER NAME REMOVED | * Identify key stakeholders and help make sure they attend relevant meetings and workshops. * Facilitate communication and requests for information from the Microsoft team. * Make decisions when options are presented. * Review and approve documentation produced by Microsoft as required. |

### Build

During the Build phase, the team refines the baseline design created in the Plan phase and builds and tests the solution. Completion of this phase marks the transition to the Stabilisation phase.

Table 32: ESAE - Build phase

|  |  |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | * Implement ESAE in the Test environment (dedicated secure room). * Establish ESAE build definitions for all solution components in scope. * Create the Test Guide document and review with CUSTOMER NAME REMOVED . * Document the build process in the Implementation Guide document and review with CUSTOMER NAME REMOVED . |
| **CUSTOMER NAME REMOVED activities** The activities to be performed by CUSTOMER NAME REMOVED | * Provide a security-enhanced room for the Test environment and implement any procedural requirements to build servers in a security-enhanced room. * Participate in Build activities. |

### Stabilise

During the Stabilise phase, testing is conducted, and the team focuses on resolving problems and bugs to prepare the solution for release. Then the solution is ready for deployment.

Table 33: ESAE - Stabilise phase

|  |  |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | * Assist with system testing activities. * Create the Operations Guide document and review with CUSTOMER NAME REMOVED. |
| **CUSTOMER NAME REMOVED** **activities** The activities to be performed by CUSTOMER NAME REMOVED | * Prepare test data and CUSTOMER NAME REMOVED specific tests. * Perform system testing, with the following estimated durations:   + - 1 day for onboarding users.     - 2 days to implement test guide.     - 5 days to implement CUSTOMER NAME REMOVED specific tests. * Review, acceptance, and approval of the operations guide document. |

### Deploy

During the Deploy phase, the team conducts the activities needed to deliver the solution.

Table 34: ESAE - Deploy Phase

|  |  |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | * Assist with moving ESAE from the Test environment to the datacentre and connecting it to the Production environment. * Configure in-scope Domain controllers for the ESAE environment per domain for up to ten (10) domains sequentially * Provide support for additional in-scope Domain controllers being configured for the ESAE environment. * Support CUSTOMER NAME REMOVED acceptance testing. * Conduct project closeout. |
| **CUSTOMER NAME REMOVED** **activities** The activities to be performed by CUSTOMER NAME REMOVED | * Put the Implementation Guide into effect to move ESAE to the Production environment and connect it. * Configure any additional Domain controllers for the ESAE environment. * Remove existing members from the Domain Admins group in all production domains managed by ESAE. * Perform CUSTOMER NAME REMOVED acceptance testing. * Implement required change control processes. |
| Key assumptions | CUSTOMER NAME REMOVED team will shadow the Microsoft team to develop internal capability for any additional forest, domain, or DC deployments. |

## Deliverables

This section provides a list of the deliverables produced by the ESAE project. If a deliverable requires formal review and acceptance (indicated by a Yes), it will be governed by the deliverable acceptance process as defined in section 2.5.

Table 35: ESAE – Deliverables

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Phase | Deliverable name | Deliverable Description | Acceptance Required | Responsibility |
| D10 | Envision | ESAE Vision and Scope Document | Microsoft Word document describing the technical architecture of the solution | Yes  Acceptance Criteria:  A Microsoft Word document of approximately 20 to 50 pages, that contains the information agreed during the Envisioning workshop. | Microsoft |
| D11 | Plan | Architecture and Design document | Word document describing the physical architecture of the ESAE solution. | Yes  Acceptance Criteria:  A Microsoft Word document of approximately 100 to 130 pages, that accurately describes the solution design | Microsoft |
| D12 | Build | ESAE Test Environment | ESAE implemented in the Test environment’s security-enhanced room. | No | Microsoft |
| D13 | Build | Test Guide Document | Word document describing how to test the ESAE | No | Microsoft |
| D14 | Build | Implementation Guide document | Word document describing how to build the ESAE environment inside of CUSTOMER NAME REMOVED environment. | Yes  Acceptance Criteria:  A Microsoft Word document of approximately 100 to 130 pages, that accurately describes the steps to build the solution | Microsoft |
| D15 | Stabilise | Operations Guide document | Word document describing operational procedures for using the ESAE solution in production. | No | Microsoft |
| D16 | Deploy | Production ESAE deployment | Implement production deployment of ESAE based on the Implementation Guide. | No | CUSTOMER NAME REMOVED |

## Project roles and responsibilities

The key project roles and the responsibilities are as follows.

### CUSTOMER NAME REMOVED

Required CUSTOMER NAME REMOVED Roles are defined at the Program level in section 3.2.1.

### Microsoft

Table 36: ESAE - Project roles and responsibilities - Microsoft

|  |  |  |
| --- | --- | --- |
| Role | Responsibilities | |
| ESAE Consultant(s) | * Technical design leadership. * Delivery of all workshops and sessions. * Development of technical deliverables. |

# P03: Privileged Access Workstation (PAW) – Tier 1

## Objectives

This project focuses on three major outcomes for the target workload:

* Assess and adapt the Microsoft Active Directory Administration Model specifically to provide security controls and hardening restrictions to the tier 1 server workloads (not the installed applications, only the server OS).
* Deploy a Privileged Access Workstation (PAW) specific to that workload(s) to protect the privileged credentials that are used to manage the workload.
* Assess and deploy Privileged Access Workstations (PAW) to be used in conjunction with the inflight PAM platform as the trusted administrative source (clean keyboard model)
  + Up to ten (10) workloads are in scope, it is assumed that of these ten (10); five (5) will be stand alone agreed upon high value assets and the remaining five (5) are Privileged Access Workstations (PAW)s configured to work in conjunction with the in-flight PAM solution

Privileged Access Workstation (PAW) is a highly controlled and managed administrative workstation that strictly controls the specific user account (role) and the specific administrative tools to only be used from this dedication hardened system to access and manage the target server workload. This hardening and control are part of the Microsoft Active Directory Administration Model set of controls, as part of this project Microsoft will:

* Support CUSTOMER NAME REMOVED with the expansion of the Tier 1 administrative model that consists of secured Group Policy Objects (GPOs), Organisation Units (OUs), and Security Groups to provide a compartmentalisation model respective of the Tier 1 security methodology – referred to as “Secure Zone” in this SOW.
* Implement up to ten (10) Tier 1 secure zones to harden High Value Asset workloads as agreed during envisioning.
* The inclusion of ten (10) workloads is to support CUSTOMER NAME REMOVED with a strong protection against high value assets such as the SWIFT banking platforms and setting the baseline protections and processes to continue with the Tier 1 hardening
* Reduce the risk of administrative credential theft by reducing the exposure of administrative workstations through the deployment of Privileged Access Workstations (PAW)s.
* Implement up to ten (10) PAW workstations, one (1) per Secure Zone.

Microsoft recommends the following type of Microsoft based workloads for consideration, non-Microsoft workloads will be discussed and agreed during envisioning.

* SQL Server
* System Center – Configuration Manager management for Windows 10
* System Center – Configuration Manager management for Server 2016 or newer
* System Center Operations Manager (SCOM)
* VMware V-Center
* SWIFT banking Windows server platform
* Trusted administrative system in conjunction with PAM solutions such as CyberArc

PAW uses the latest version of Windows 10 security functions such as:

* Windows BitLocker Drive Encryption.
* Windows App Locker.
* Windows Defender Antivirus.
* Windows Defender Credential Guard.
* Integration with Azure Log Analytics (OMS).

Basic administrative tools, such as the following, will be included in the workstation image as needed:

* Microsoft Remote Server Administration Tools (RSAT).
* Windows PowerShell.
* SQL Management Consoles.
* System Center management consoles.

## Areas in scope

### General project scope

Microsoft will provide Services in support of the following scope.

Table 37: PAW T1 – General project scope

|  |  |  |
| --- | --- | --- |
| Area | Description | Assumptions |
| PAW Tier 1 kick-off and solution workshop | * Microsoft will lead envisioning workshops that captures specific CUSTOMER NAME REMOVED environment information and defines major design decisions and the agreed workloads to be included. | * The vision and scope of the project will be documented as part of the architecture and design document * Up to three (3) days of envisioning workshops will be conducted |
| Active Directory Tier 1 Expansion | * Active Directory Administration Model configurations to support the deployment of PAW * Microsoft will support CUSTOMER NAME REMOVED to deploy:   + - The Organisational Units (OUs)     - The Group Policy Objects (GPOs)     - Grant permissions for the PAW images in production AD DS     - Support CUSTOMER NAME REMOVED with the expansion of the Tier 1 administrative security model that consists of secured Group Policy Objects (GPOs), Organisation Units (OUs), and Security Groups to provide a compartmentalisation model (Secure Zone) to:     - Apply restrictive security controls to the Windows Server OS of the target workload     - Support the deployment of a PAW for administration of the target workload     - Support the Implementation up to ten (10) Tier 1 secure zones to harden a High Value Asset workload per zone. * Development of the Tier 1 Reference Guide | * AD DS configuration is based on the Tier 1 adaptions from the ADH P01 project. * Assessment and adaption of the Microsoft’s Active Directory Administration model is time boxed to up to forty (40) hours. * Expansion of the Tier 1 administrative model will use the predefined OU’s, GPO, and Security Groups model with limited customisation as agreed by the project team. * A Secure Zone will consist of no more than:   + - Up to three (3) security groups     - Up to three (3) duplicated GPO’s     - GPO’s will be duplicated from the existing deployed reference GPO’s and modified as needed     - Up to two (2) administrative users accounts * A High Value Asset workload is defined as a logical grouping of systems that has significant importance to the business or security posture * Microsoft will support CUSTOMER NAME REMOVED with the assessment and configuration of the restrictive security controls to server assets for up to One-Hundred and Twenty (120) hours per agreed in-scope workload |
| PAW design | * Microsoft will adapt the PAW reference architecture to fit the CUSTOMER NAME REMOVED environment based on the Tier 1 extension model * Design and deployment of one (1) PAW for each of the ten (10) “Security Zones” which contain a single High Value Asset | * Based on the Microsoft Services PAW reference architecture and design * PAW will be deployed as a trusted source in the trust chain and will be a physical machine * This effort is timeboxed to three (3) days per security zone. |
| PAW administrative workstation image | * Support CUSTOMER NAME REMOVED with adapting the PAW reference architecture to support PAW in a virtualised deployment on the physical deployed PAW * Support CUSTOMER NAME REMOVED with the integration of 3rd party VPN into the PAW workstation image * Configuration of Administrative workstation deployment * One base administrative workstation image for Windows 10 will be prepared with Microsoft Deployment Toolkit (MDT) | * Configuration of two (2) physical workstation images with up to two (2) administrative application each * If the chosen workload does not comply with the restrictive templates, then an alternative workload will be chosen or managed through change management * Administrative application development is timeboxed to three (3) days per security zone. * Virtual PAW is a variation of the full PAW architecture; which the associated risk will be articulated and accepted by CUSTOMER NAME REMOVED prior to adapting the reference architecture to a virtualisation platform * Virtual “PAWS” will strictly be deployed only to a physical PAW and on the Hyper-V hypervisor * VPN integration will be limited to the physical PAW workstation image * CUSTOMER NAME REMOVED is responsible for the 3rd party VPN design and deployment * Administrative workstation image(s) for Windows 10 Enterprise x64 will be prepared using the Microsoft Deployment Toolkit (MDT) * CUSTOMER NAME REMOVED will have the workstation hardware ready for deployment * Deployment of up to ten (10) physical Privileged Access Workstations, one (1) per security zone |
| Smart card configuration | * Design, configure, and deploy up to ten (10) CUSTOMER NAME REMOVED supplied smart cards to administrators. | * One (1) type of smart card will be used. * Smart cards are compatible with the Microsoft Base Smart Card Cryptographic Service Provider standard. |
| Monitoring | * PAWs integrate with Azure Log Analytics | * CUSTOMER NAME REMOVED is responsible for the Log Analytics Workspace |
| System testing | * PAW solution item testing rendered to CUSTOMER NAME REMOVED (applies to items within the nonproduction build environment) * System testing focuses on the functionality meeting the design. | * This is time-boxed to two (2) days. |
| User Acceptance testing assistance | * PAW solution item testing assistance rendered to CUSTOMER NAME REMOVED (applies to items within the nonproduction build environment) * System testing focuses on the functionality meeting the design. | * This is time-boxed to one (1) day |

### Software products and technologies

The products and technology that are listed in the following table are required for project execution. CUSTOMER NAME REMOVED is responsible for obtaining all identified licenses and products.

Table 38: PAW T1 – Software products and technologies

|  |  |  |
| --- | --- | --- |
| Product and technology item | Version | Ready by |
| Microsoft Windows Server | 2016 | Project start |
| Microsoft Windows | 10 Enterprise x64 | Project start |

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

Table 39: PAW T1 – Other software products and technologies

|  |  |
| --- | --- |
| Product and technology item | Ready by |
| Microsoft BgInfo (from the Sysinternals Suite) | Scripted download |
| Microsoft Assessment and Deployment Kit | Scripted download |
| Windows Management Framework | Scripted download |
| Microsoft Report Viewer | Scripted download |
| Microsoft Deployment Toolkit | Scripted download |
| Microsoft .NET Framework | Scripted download |
| Microsoft Attack Surface Analyzer | Scripted download |
| Microsoft Network Monitor | Scripted download |
| Microsoft Message Analyzer | Scripted download |
| RSAT for Windows | Scripted download |
| Microsoft LAPS | Scripted download |
| TCPView for Windows (from the Sysinternals Suite) | Scripted download |
| Microsoft Process Explorer (from the Sysinternals Suite) | Scripted download |
| Microsoft Process Monitor (from the Sysinternals Suite) | Scripted download |
| Microsoft PsTools (from the Sysinternals Suite) | Scripted download |
| Administrative templates for Windows 10 | Scripted download |

### System integration

The following system integration is in scope for the project:

Table 40: PAW T1 – System integration

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Integration | Description of scope | Responsibility | | Ready by |
| Production AD DS | * AD DS membership - The PAWs will be joined to the CUSTOMER NAME REMOVED production domain. * AD DS configuration - OUs, GPOs and delegated permissions will be added to the production AD DS service. | CUSTOMER NAME REMOVED | Start of the project | |

### Environments

The following table provides information about the development and test facilities that are to be used by the project team members. For the following environments, CUSTOMER NAME REMOVED will be responsible for allocating and setting up the base hardware, network hardware and network connectivity and will provide the required software. The joint Microsoft and CUSTOMER NAME REMOVED team will install and configure the software products shown in Section 7.2.2 of this document.

Table 41: PAW T1 – Environments

|  |  |  |  |
| --- | --- | --- | --- |
| Environment | Location | Responsibility | Ready by |
| Production | Secure datacentre | CUSTOMER NAME REMOVED | Before the Deploy phase of this project |

### Testing

The following testing will be performed.

Table 42: PAW T1 – Testing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test type (environment) | Description | Responsibility | | |
| Has responsibility  for testing? | Provides data or test cases | Provides guidance and support |
| System testing  (Production) | System testing focuses on the functionality meeting the design. The testing duration is time-boxed to two (2) days. Test cases are based on the test plan. | Microsoft | Microsoft and CUSTOMER NAME REMOVED | CUSTOMER NAME REMOVED |
| User acceptance testing  (Production) | This consists of testing administrator functionality of key real-world scenarios. Testing duration is time-boxed to one (1) day. Test cases are based on the operations guide. | CUSTOMER NAME REMOVED | CUSTOMER NAME REMOVED | Microsoft |

## Areas out of scope

Any area not explicitly included in the Areas in scope section is out of scope for Microsoft during this project. Areas out of scope for this project, in addition to those listed elsewhere in this document, are listed in the following table.

Table 43: PAW T1 – Out of scope

|  |  |  |
| --- | --- | --- |
| Area | Description | |
| PAW enterprise functions | * Windows 10 Enterprise functionalities such as Internet Protocol Security (IPsec), Windows Device Guard. |
| Discovery | * Discovery and categorisation of administrative tasks and applications. |
| Cloud services planning | * Planning for cloud services such as Microsoft Azure and Microsoft Azure Active Directory. |
| Log Analytics (OMS) configuration | * Configuration of Log Analytics dashboards, reports, or related items beyond onboarding the PAWs. |
| Older operating systems | * Support for PAWs using operating system versions or image configurations other than those included in the project scope. |
| General production domain hardening | * Securing of AD DS components other than privileged user accounts. General hardening of servers such as domain controllers is out of scope. |
| Process re-engineering | * Design of functional business components of the solution unless specifically included in scope and delivered by MCS Operations Consulting staff. |
| Organisational Change Management | * Design or re-design of CUSTOMER NAME REMOVED’s functional organisation unless specifically included in scope and delivered by MCS Operations Consulting staff. |

## Approach

This project will be structured following the Microsoft Solutions Framework methodology, which consists of five phases: Envision, Plan, Build, Stabilise and Deploy. Each phase has distinct activities that are described in the following sections.

Figure 9: PSW T1 – Approach

Envision

Plan

Build

Stabilise

Deploy

### Envision

During the Envision phase Microsoft and CUSTOMER NAME REMOVED will reach agreement on a shared vision for the project and the specific scope that will be required to make that vision a reality.

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

Table 44: PAW T1 – Envision activities

|  |  |  |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | * Conduct Kick-off meeting. * Design sessions covering conceptual PAW reference architecture. * Assist in determining mutually agreed Vision and Scope items. * Update project schedule as required. |
| **CUSTOMER NAME REMOVED activities** The activities to be performed by CUSTOMER NAME REMOVED | * Gather information that might be requested during the Envision workshop. * Make decisions when architectural options are presented. * Engage operations and service owners to help raise awareness about systems to be implemented. |
| Key assumptions | * CUSTOMER NAME REMOVED service owners and architects have been identified and can attend and participate in the PAW envisioning workshop. * Current configuration and data descriptions are available. |

### Plan

During the Plan phase, Microsoft will work with CUSTOMER NAME REMOVED to develop and meet the technical and functional requirements in the logical and physical designs and to define and describe the environment end state. The program plan will also be updated to reflect the detailed timeline for the Build, Stabilise and Deploy phases of this project.

Table 45: PAW T1 – Plan activities

|  |  |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | * Assessment and adaption of the Microsoft’s Reference Architecture for Active Directory Administration for Tier 1; up to forty (40) hours per domain in scope. * Support the deployment of the user rights assignment assessment tools * Development of the Tier 1 Reference Guide. * Review of the reference model GPO’s, OU’s and Security Group structure with the project team. * Update to the Architecture and design document with CUSTOMER NAME REMOVED environment information. |
| **CUSTOMER NAME REMOVED activities** The activities to be performed by CUSTOMER NAME REMOVED | * Gather information that might be requested during the Planning design sessions. * Review the architecture and design document and participate in its approval. * CUSTOMER NAME REMOVED subject matter experts (SMEs) will participate in the design sessions and make decisions when architectural options are presented. |
| Key assumptions | PAW Tier 1 reference architecture can be deployed in the CUSTOMER NAME REMOVED environment |

### Build

During the Build phase, the team builds the solution in production unlinked and isolated from the rest of the directory. The goal of this phase is to support the team with extending the Tier 1 model to the production Active Directory environment.

Table 46: PAW T1 – Build activities

|  |  |  |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | * Assist CUSTOMER NAME REMOVED in implementing the recommended AD DS administration model into the target production AD DS domains in scope. * Support CUSTOMER NAME REMOVED with the expansion of the Tier 1 administrative model; up to twenty-four (24) hours * Support CUSTOMER NAME REMOVED with the implementation of up to ten (10) Security zones to harden up to a single High Value Asset (1) per zone * Deploy a PAW image up to ten (10) production workstations that are attached to a simulated production AD DS. * Deploy a virtual PAW image up to one (1) production workstations that are attached to a simulated production AD DS. * Update Test guide document. * Review Test guide document with CUSTOMER NAME REMOVED. * Update Implementation guide document. * Review Implementation guide document with CUSTOMER NAME REMOVED. |
| **CUSTOMER NAME REMOVED activities** The activities to be performed by CUSTOMER NAME REMOVED | * Participate in Build activities. * Participate in the review activities. * Provide staff for information needed for Phase deliverables. |
| Key assumptions | * CUSTOMER NAME REMOVED SMEs will participate in the development sessions. * CUSTOMER NAME REMOVED will provide appropriate secure room facilities, including hardware and software. * CUSTOMER NAME REMOVED will provide CUSTOMER NAME REMOVED specific test cases. |

### Stabilise

During the Stabilise phase, the combined Microsoft and CUSTOMER NAME REMOVED team will implement the test plan, document the results for the test cases and validate the Build process. Microsoft will record the recommended operational practices and procedures in the operations guide.

The Stabilise phase ends when the solution has been verified through the implementation of the test plan by CUSTOMER NAME REMOVED.

Table 47: PAW T1 – Stabilise activities

|  |  |  |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | Functional test using the test cases from the test plan. Up to two (2) days per domain in scope.   * Update Operations guide document. * Review Operations guide with CUSTOMER NAME REMOVED. |
| **CUSTOMER NAME REMOVED activities** The activities to be performed by CUSTOMER NAME REMOVED | * Engage designated test users. * Perform system testing based on the test plan. |
| Key assumptions | * CUSTOMER NAME REMOVED SMEs and test users are ready to participate in the testing activities. * A post deployment support process will be established by CUSTOMER NAME REMOVED prior to commencement of the Deploy phase. |

### Deploy

The Deploy phase begins with the implementation of the PAW solution for production use and ends with the deployment of the Tier 1 PAWs into production.

Table 48: PAW T1 – Deploy activities

|  |  |  |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | * Support CUSTOMER NAME REMOVED with the implementation of the security zones * Connecting PAW to the production environment   + - During PAW production implementation, Microsoft will assist as needed as CUSTOMER NAME REMOVED puts the implementation guide into effect.     - Microsoft support activities are limited to the first ten (10) PAWs in the CUSTOMER NAME REMOVED production domains in scope. * Handover and closeout of the project. |
| **CUSTOMER NAME REMOVED activities** The activities to be performed by CUSTOMER NAME REMOVED | * Deploy the solution to production * Provide direction to the Microsoft resources during this project phase * Run CUSTOMER NAME REMOVED acceptance tests * Provide feedback on production use * Provide sign-off for project results |
| Key assumptions | * CUSTOMER NAME REMOVED will take responsibility for its change control processes. * Affected organisations will identify the resources and groups that will be required for the Deploy phase. |

## Deliverables

This section provides a list of the deliverables produced by the PAW T1 project. If a deliverable requires formal review and acceptance (indicated by a Yes), it will be governed by the deliverable acceptance process as defined in section 2.5.

Table 49: PAW T1 – Deliverables

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Phase | Deliverable name | Deliverable Description | Acceptance Required | Responsibility |
| D17 | Plan | PAW T1 Architecture and design document | Microsoft Word Document with PAW reference architecture including description of the solution and its components, logical solution and physical implementation. | Yes  Acceptance Criteria:  A Microsoft Word document of approximately 100 to 130 pages, that accurately describes the solution design | Microsoft |
| D18 | Build | PAW T1 Implementation guide document | Microsoft Word document with configuration information and step by step instructions used to build the end-state that has been described in the architecture and design document. | No | Microsoft |
| D19 | Build | PAW T1 Test guide | Microsoft Word document with test cases documenting testing procedures. | No | Microsoft |
| D20 | Stabilise | PAW T1 Operations guide document | Microsoft Word document with operational guidance for the systems and components that are described in the architecture and design document. | No | Microsoft |
| D21 | Deploy | Up to ten (10) production PAWs deployed | Up to ten (10) production PAWs have been successfully deployed and tested. | No | Microsoft |

## Project roles and responsibilities

The key project roles and the responsibilities are as follows.

### CUSTOMER NAME REMOVED

Required CUSTOMER NAME REMOVED Roles are defined at the Program level in section 3.2.1.

### Microsoft

Table 50: PAW T1 – Microsoft roles and responsibilities

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Responsibilities | Project Commitment | |
| PAW Consultant | * Provide technical design leadership * Deliver workshops and sessions * Responsible for development of technical deliverables | * Full time |

## CUSTOMER NAME REMOVED responsibilities

In addition to CUSTOMER NAME REMOVED activities defined in the Approach section, CUSTOMER NAME REMOVED is also required to:

* Provide a dedicated physically secure room with desks, chairs and network access that the project team can use for the duration of the project (should be ready before the project kick off):
  + - * Six (6) unused and unopened laptops or desktops that will be used as production PAWs
* Provide access to the Azure subscription used to monitor PAWs.

## Project assumption

Microsoft will support CUSTOMER NAME REMOVED with the initial deployment of PAW T1 as defined in Areas in scope, however CUSTOMER NAME REMOVED will need to continue this process for the remainder of the environment and as part of their ongoing operational maintenance and administration activities.

# P04: Azure Security Foundations (ASF)

## Objectives

Cloud identities are just as critical and vulnerable to attack as the identities on-premises. Managing the identities for any cloud workload is the last mile responsibility of the bank as such due diligence to wrap the same security controls and restrictions to these highly privileged accounts is critical.

The bank has an extensive Azure deployment and existing Role Based Access (RBAC) model to manage identities in the Azure platform. This workstream is focused only on the highest privileged credentials that sit atop this existing RBAC model and are in full control of the Azure cloud tenants. The goal is to provide highly secured controls and security restrictions to the highly privileged accounts and support the reduction of exposure of these accounts

Design and build the component services and features that will support a robust security protection of cloud-based identities and Azure platform focused on the core privileged identities that manage and control the cloud platform.

The component services and features to achieve this are;

* Azure Role Based Access Control (RBAC)
* Azure Identity Protection
* Azure Security Policies
* Azure Privilege Identity Management
* Conditional access

## Areas in scope

### General project scope

Microsoft will provide Services in support of the following scope.

Table 51: ASF - General project scope

|  |  |  |
| --- | --- | --- |
| Area | Description | Assumptions |
| Workshops | Microsoft will assist CUSTOMER NAME REMOVED by conducting workshops covering the following topics for up to forty (40) hours:   * Azure Security Policies * Azure Identity protection features covering protection, detection and response capabilities * Azure RBAC * Privilege Identity Management | * Key decision makers will participate in the workshop, provide security requirements and make timely decisions relevant to this area. * Up to six (6) separate Azure tenants, each with up to one (1) subscription per tenant are in scope. * Up to six (6) accounts in scope in each in scope tenant include: * Global Administrators * Subscription Administrators * Billing Administrators * Accounts that have equivalent privileges to any of the above listed accounts |
| Azure Policies | Microsoft will assist CUSTOMER NAME REMOVED by providing planning and configuration assistance for up to five (5) Security Policies for the tenants in scope. | * CUSTOMER NAME REMOVED will provide their requirements. |
| Azure Identity Protection configuration | Microsoft will assist CUSTOMER NAME REMOVED by providing planning and configuration assistance for up to sixteen (16) hours per in scope tenant:   * Azure Identity protection security policies * Identity protection roles * Configuring Multi Factor Authentication (MFA) and conditional access for cloud privileged identities * Demonstrating how to detect and respond to identity related security events. | * CUSTOMER NAME REMOVED will provision Azure based privileged identities. |
| Azure Privilege Identity Management | Microsoft will assist CUSTOMER NAME REMOVED by providing planning and configuration assistance for the following in each in scope tenant:   * Enabling PIM for up to five (5) highly privileged administrative roles in Azure AD * Enabling PIM for up to five (5) privilege roles for managing Azure resources. | * CUSTOMER NAME REMOVED has valid Azure AD Premium P2 or trial license for each user that interacts with Azure PIM service. |
| RBAC | Microsoft will assist CUSTOMER NAME REMOVED with the following in each in scope tenant:   * Defining RBAC model for Azure platform * Configuring up to five (5) RBAC roles that use built-in Azure RBAC role definitions | * CUSTOMER NAME REMOVED will provide RBAC requirements and their operating model. * Configure up to six (6) Azure subscriptions and administrators * CUSTOMER NAME REMOVED will be responsible for scaling RBAC to any other subscriptions and resources outside the limits of current scope of work |

## Areas out of scope

Any area not explicitly included in the areas in scope section is out of scope for Microsoft during this project. Areas out of scope for this project, in addition to those listed elsewhere in this document, are listed in the following table.

Table 52: ASF – Out of scope

|  |  |
| --- | --- |
| Area | Description |
| Azure Active Directory Integration | * Installation and configuration of Azure Active Directory Connect * Configuration of Azure Active Directory authentication using password synchronisation, pass-through authentication, or federated authentication * Implementation of the Azure Active Directory seamless single sign-on (SSO) * Installation of the Azure Active Directory Connect Health Agent * Implementation of Azure Active Directory business-to-business (B2B) * Installation and configuration of AD FS and Web Application Proxy (WAP) roles |
| Azure Active Directory identity management | Changes to individual group objects to accommodate self-service management in Azure Active Directory, including conversion of synchronised groups to cloud-based groups, is out of scope. |
| Azure MFA server or third-party MFA providers | Deployment of the on-premises Azure MFA server is outside the scope of this project, as is integration with a third-party multi-factor authentication provider. |

## Testing

The following testing is included in the scope of this work package.

Table 53 ASF - Testing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test type (environment) | Description | Responsibility | | |
| Has responsibility  for testing? | Provides data or test cases | Provides guidance and support |
| System and Functional testing (Enable) | System and Functional testing focus on validating Azure Identity and security features as mentioned in Areas in scope section.  This duration of the activity is time boxed to three (3) days per in scope tenant. | Microsoft | CUSTOMER NAME REMOVED | Microsoft |

## Approach

Microsoft will follow a structured approach for the deployment of Azure functionality and features within the Azure Security project. This approach is as follows:

* **Assess:** during the Assess phase, Microsoft works with you to begin the project and complete design and planning workshops. The result is a number of relevant designs which will be built and deployed into your production environment during the Enable phase.
* **Enable:** during the Enable phase, Microsoft works with you to prepare, deploy and validate the new services and functionality into your production network environment.

This section will provide additional detail regarding key activities and assumptions for each phase of this project.

### Assess

Pre-requisite: CUSTOMER NAME REMOVED is expected to provision/remediate any network firewall setup/changes two (2) weeks before the commencement of this Assess phase.

The Assess phase begins with the project initiation (kick-off) and ends with the completion of an AD DS design, which will be configured and deployed in the Enable phase.

Table 54: ASF - Assess phase activities

|  |  |  |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | * Conduct a one (1) day workshop per in scope tenant and facilitate requirement gathering covering following topics:   + - Azure Security Policies     - Azure Identity protection features covering protection, detection and response capabilities     - Azure RBAC     - Privilege Identity Management * Conduct meetings to review and define security requirements, specifically pertaining to Azure policies, RBAC, Privileged Identity Management and security monitoring * Plan for Azure Security Center roles and identify the scope of ASC monitoring * Develop an Azure Security and Identity design document with decisions related to Azure policies, Azure RBAC, Identity protection and ASC policies configuration * Microsoft will conduct up to five (5) Azure Security educational workshops with each workshop not exceeding four (4) hours. |
| **CUSTOMER NAME REMOVED** **activities** The activities to be performed by CUSTOMER NAME REMOVED | * Participate in workshops * Provide security requirements and decisions as necessary to enable Azure security * Review CUSTOMER NAME REMOVED ’s operating model and define RBAC and role assignment for their users |
| Key assumptions | * CUSTOMER NAME REMOVED has procured required subscriptions * As applicable, CUSTOMER NAME REMOVED will provide Microsoft with access to subscription to review their current state * Key decision makers will participate in the workshops and will share their security requirements * Key CUSTOMER NAME REMOVED stakeholders will make timely decision regarding Azure policies and role definition |

### Enable

During the Enable phase, Microsoft will provide security configuration assistance as per the design document developed in Assess phase.

Table 55: ASF - Enable phase activities

|  |  |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | * Assist with configuring up to five (5) Azure security policies per subscription for up to two (2) subscriptions. * Assist with configuring Azure Role Based Access Control (RBAC) by assigning roles to users. The assistance will be limited to defining and assigning up to five (5) built-in roles to CUSTOMER NAME REMOVED users for up to six (6) subscriptions. * Provide up to sixteen (16) hours of time boxed assistance to configure following identity security controls:   + - Define Identity Protection roles     - Enablement of MFA for identified users in AAD     - conditional access policies     - Demonstrate Azure AD logging and threat detection features |
| **CUSTOMER NAME REMOVED activities** The activities to be performed by CUSTOMER NAME REMOVED | * Provide Privileged Access workstation (PAW) or a clean secure admin workstation for Microsoft personnel to assist with security configuration. * CUSTOMER NAME REMOVED will be responsible for scaling their RBAC model based on their operational needs. * Work with Microsoft personnel during configuration. |
| Key assumptions | * CUSTOMER NAME REMOVED will provide Microsoft with required access to their subscription. |

## Deliverables

This section provides a list of the deliverables produced by the ASF project. If a deliverable requires formal review and acceptance (indicated by a Yes), it will be governed by the deliverable acceptance process as defined in section 2.5.

Table 56: ASF – Deliverables

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Phase** | **Deliverable name** | **Deliverable Description** | **Acceptance Required** | **Responsibility** |
| D22 | Assess | Azure Security Design document | Document with Azure Security components architecture including description of the solution and its components, logical solution, and implementation. | Yes  Acceptance Criteria:  A Microsoft Word document of approximately 100 to 130 pages, that accurately describes the solution design | Microsoft |
| D23 | Assess | Azure Security Preliminary System Test plan | A Test plan spreadsheet describing test cases for validating Azure security features as per Azure Security Design document | No | Microsoft |
| D24 | Enable | Azure Security Configuration demonstration | Solution Demonstration and assistance of production configuration | No | Microsoft |
| D25 | Enable | Azure Security Implementation Guide | A single document describing the security controls applied in given subscription | No | Microsoft |
| D26 | Enable | Azure Security Updated Test plan | Updated Test plan with system test results | Yes  Acceptance Criteria:  A Microsoft Word document of approximately 25 – 40 pages, that includes the expected test results and notes about implementing the defined test cases. | Microsoft |
| D27 | Enable | Azure Security Operations Guide | A single document describing the operational guidance for Azure security controls as per design document. | No | Microsoft |

## Project roles and responsibilities

The key project roles and the responsibilities are as follows.

### CUSTOMER NAME REMOVED

Required CUSTOMER NAME REMOVED Roles are defined at the Program level in section 3.2.1.

### Microsoft

Table 57: ASF - Microsoft roles and responsibilities

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Responsibilities | Project Commitment | |
| Azure Consultant | * Provide technical design leadership * Deliver workshops and sessions * Responsible for development of technical deliverables | Full time |

# P05: Azure Cloud Privileged Access Workstation (PAW)

## Objectives

As with the Privileged Access Workstation (PAW), similar cloud controlled, and managed administrative workstations are used to protect the top privileged accounts that are in control of the Azure cloud deployments. Cloud PAW leverages the same reference architecture as the on-prem version however it is fully managed and controlled by Azure security features and controls. This gives an administrative and security boundary to these cloud-based admin accounts.

* Cloud PAW reduces the risk of cloud privileged administrative credential theft by reducing the exposure of administrative workstations

The objective of the project is to implement Cloud PAWs with applications for the following administrative tasks, which are based on Microsoft-recommended practices, architectures, accumulated field experience, and CUSTOMER NAME REMOVED requirements such as:

* Azure Active Directory
* Azure Administrative Portal
* Office 365 Administrative Portal

Cloud PAW leverages the newest and most advanced security features in the Azure Security suite of products and Windows 10 Enterprise, including:

* Unified Extensible Firmware Interface (EFI) Secure Boot
* Windows BitLocker Drive Encryption
* Windows Defender Antivirus
* Windows Defender Credential Guard
* Windows Defender Exploit Guard
* Windows Defender Firewall
* Windows Defender Application Control (WDAC)
* Integration with Azure Log Analytics
* Intune compliance and configuration policy
* Azure Active Directory Conditional Access
* Windows Defender ATP
* Azure Active Directory Identity Protection
* Azure Active Directory PIM
* Azure Active Directory Delegation of Admin design

## Areas in scope

This section details the areas which are within scope.

### General project scope

Microsoft will provide Services in support of the following scope.

Table 58: PAW – General project scope

|  |  |  |
| --- | --- | --- |
| Area | Description | Assumptions |
| Cloud PAW kick-off and solution workshop | Microsoft will lead a one (1) day workshop during which the team kicks off the project, documents specific CUSTOMER NAME REMOVED environment information and agree on the major design decisions with CUSTOMER NAME REMOVED. | * The vision and scope of the project will be documented as part of the architecture and design document. * Up to six (6) separate Azure tenants, each with up to one (1) subscription per tenant are in scope. * Up to six (6) Azure Cloud PAW’s are in scope. |
| Cloud PAW reference architecture - Azure Active Directory Security Services | Microsoft will use the Cloud PAW reference architecture including the following:   * Intune compliance and configuration policy * Azure Active Directory Conditional Access * Windows Defender ATP * Azure Active Directory Identity Protection * Azure Active Directory PIM * Windows Defender Device Guard * White listing * Host based security * BitLocker * Azure Active Directory Delegation of Admin design * MDT – Task Sequence to deploy Clean Source to device to include: * PowerShell modules for Azure Resource Manager * PowerShell modules for Azure Active Directory * PowerShell modules for Office 365 | * Cloud PAW reference architecture can be deployed in the CUSTOMER NAME REMOVED Azure Tenant as is, without modification. * E5 license required for Cloud Paw administrators |
| Cloud PAW administrative workstation image | * Configure a single workstation image for one (1) hardware model or type * One administrative workstation image for Windows 10 Enterprise will be prepared with the Microsoft Deployment Toolkit (MDT). * Support CUSTOMER NAME REMOVED with the integration of Azure Point-to-Site VPN or 3rd party VPN solution into the PAW workstation image * This image is designed for one (1) specific set of administrative applications:   + - Azure Administrative Portal     - Azure Active Directory Administration Portal     - Office 365 Administrative portal * Any supporting portal required to manage the above * This effort is time-boxed to three (3) days per in scope tenant. |  |
| Administrative workstation deployment | Deploy up to one (1) Cloud PAWs per in scope tenant. | CUSTOMER NAME REMOVED will have the workstation hardware ready before the start of the project. |
| Monitoring | Cloud PAW integration with Azure Log Analytics. | CUSTOMER NAME REMOVED has an Azure subscription and Log Analytics workspace ready before the project starts. |
| System testing assistance | * Cloud PAW solution item testing assistance rendered to CUSTOMER NAME REMOVED (applies to items within the nonproduction build environment) * System testing focuses on the functionality meeting the design. * This is time-boxed to two (2) days. | Testing assistance is constrained to the time allocated during this project. |
| One deployment | * Cloud PAWs will be deployed in a physically secure room and connected to the Azure Active Directory Tenant * After testing is complete, the solution will be moved from the secure room to an agreed upon production location, secured and controlled. | The physically secure room that contains the server hardware will be ready before the project starts. |

### Software products and technologies

The products and technology which are listed in the following table are required for the project. CUSTOMER NAME REMOVED is responsible for obtaining all identified licenses and products.

Table 59: PAW - Software products and technologies

|  |  |  |
| --- | --- | --- |
| Product and technology item | Version | Ready by |
| Windows Server | 2016 or newer | Start of the project |
| Windows | 10 Enterprise x64 | Start of the project |
| E5 License | Current | Start of the project |

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

Table 60: PAW - Software packages required

|  |  |
| --- | --- |
| Product and technology item | Ready by |
| Microsoft BGInfo (from the Sysinternals Suite) | Scripted download |
| Microsoft Assessment and Deployment Kit (ADK) | Scripted download |
| Windows Management Framework | Scripted download |
| Microsoft Report Viewer | Scripted download |
| Microsoft Deployment Toolkit (MDT) | Scripted download |
| Azure PowerShell modules | Scripted Download |
| Office 365 PowerShell Modules | Scripted Download |

### System integration

The following system integration is in scope for the project.

Table 61: PAW - System integration in scope

|  |  |  |  |
| --- | --- | --- | --- |
| Integration | Description of scope | Responsibility | Ready by |
| Secure Room | * Cloud PAWs will be deployed in a physically secure room and connected to the Azure Active Directory Tenant | CUSTOMER NAME REMOVED | Start of the project |
| Production Azure Active Directory Tenant | * The production Azure Active Directory Tenant | CUSTOMER NAME REMOVED | Start of the project |

### Environments

The following table provides information about the development and test facilities which are to be used by the project team members. For the following environments, CUSTOMER NAME REMOVED will be responsible for allocating and setting up the base hardware, network hardware, and network connectivity, and will provide the required software. The joint Microsoft and CUSTOMER NAME REMOVED team will install and configure the software products shown in the Software products and technologies section of this document.

Table 62: PAW - Environments

|  |  |  |  |
| --- | --- | --- | --- |
| Environment | Location | Responsibility | Ready by |
| Build | Dedicated secure room | CUSTOMER NAME REMOVED | Before the Build phase of this project |
| Production | Secure datacentre/location | CUSTOMER NAME REMOVED | Before the Deploy phase of this project |
| Log Analytics Workspace | Azure Tenant | CUSTOMER NAME REMOVED | Before the Build phase of this project |
| Azure Active Directory Tenant | Azure Tenant | CUSTOMER NAME REMOVED | Before the Build phase of this project |
| Intune | Azure Tenant | CUSTOMER NAME REMOVED | Before the Build phase of this project |
| Windows Defender ATP | ATP Workspace | CUSTOMER NAME REMOVED | Before the Build phase of this project |
| Firewalls  Internet connectivity  Domain Name Service (DNS)  Active Directory Certificate Services | Azure Tenant | CUSTOMER NAME REMOVED | One week prior to production deployment |

### Testing and defect remediation

#### Testing

The following testing is included in the scope of the project. If CUSTOMER NAME REMOVED has responsibility for testing, the Microsoft effort to support that activity is identified. If additional time is needed for Microsoft testing support, then it can be requested through the Change Management Process described in this SOW.

Table 63: PAW - Testing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test type (environment) | Description | Responsibility | | |
| Has responsibility  for testing? | Provides data or test cases | Provides guidance and support |
| System testing (build) | System testing focuses on the functionality meeting the design. The testing duration is time-boxed to two (2) days. Test cases are based on the test guide. | Microsoft | CUSTOMER NAME REMOVED | Microsoft |
| CUSTOMER NAME REMOVED acceptance testing (production) | This consists of testing administrator functionality of key real-world scenarios. Test cases are based on the operations guide. Testing duration is time-boxed to one (1) day. | CUSTOMER NAME REMOVED | CUSTOMER NAME REMOVED | Microsoft |

## Areas out of scope

Any area not explicitly included in the areas in scope section is out of scope for Microsoft during this project. Areas out of scope for this project are listed in the following table.

Table 64: PAW - Out of scope

|  |  |  |
| --- | --- | --- |
| Area | Description | |
| Cloud PAW enterprise functions | Windows 10 Enterprise functionalities such as Internet Protocol Security (IPsec), smart card logon, and Windows Defender Application Guard. |
| Cloud PAW as a virtual machine | Deploying one (1) or multiple Cloud PAWs and productivity workstation as virtual machines (unless added as an option to this engagement). | |
| Discovery | Discovery and categorisation of administrative tasks and applications. |
| Multiple domain or forest support | Support for more than one (1) Azure Tenant. |
| Role definition | Custom definition of roles and the creation of new accounts or roles (such as groups). |
| Log Analytics (OMS) configuration | Configuration of Log Analytics dashboards, reports, or related items beyond onboarding the Cloud PAWs. |
| Remote access for Cloud PAWs | * Implementation or configuration of third-party VPN gateways or Remote Authentication Dial-In User Service (RADIUS) servers. * Implementation or configuration of third-party authentication systems or other networking components. * Implementation or configuration of AD CS. * Configuration of DNS, third-party authentication systems, edge/perimeter firewalls, hardware load balancers, global server load balancers, or other networking components. |

## Project approach

This chapter details the Cloud PAW project approach.

### Approach

This project follows the Online Services Lifecycle methodology, and work is divided into 3 distinct phases: Assess, Remediate, and Enable. Each phase has distinct activities which are described in the following sections.



Figure 10: Azure Cloud PAW - Approach

#### Assess

During the Assess phase, Microsoft will work with you to begin the project and complete the design and planning workshops. The result is an Azure Cloud PAW design that will be built, deployed, and configured into your production environment during the Enable phase.

Table 65: PAW - Assess phase

|  |  |
| --- | --- |
| Category | Description |
| Microsoft activities The activities to be performed by Microsoft | * The design sessions will cover conceptual Cloud PAW reference architecture. * Agree on the requirements and scope and document them in the Technical Guide. * Update the technical guide document with CUSTOMER NAME REMOVED environment information. * Review the technical guide with CUSTOMER NAME REMOVED.   Update program plan with key milestones. |
| CUSTOMER NAME REMOVED activities  The activities to be performed by CUSTOMER NAME REMOVED | * Gather information which might be requested during the requirements and planning workshops. * Review the design document deliverable and participate in its approval process. * Make decisions when architectural options are presented. * Engage operations and service owners to help raise awareness about systems to be implemented. * Review the implementation guide and participate in its approval. * CUSTOMER NAME REMOVED subject matter experts (SMEs) will participate in the design sessions and make decisions when architectural options are presented. |
| **Key assumptions** | * CUSTOMER NAME REMOVED service owners and architects have been identified and will attend and participate in the Cloud PAW workshops. * Cloud PAW reference architecture can be deployed in CUSTOMER NAME REMOVED environment as-is, without modification. |

#### Remediate

During the Remediate phase, the team will resolve or mitigate all items in the remediation checklist that was developed during the remediation planning workshop in the Assess phase.

Table 66: PAW - Remediate phase

|  |  |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | Build the MDT server used to deploy Cloud PAWs.   * Deploy the Intune compliance and configuration policy * Deploy the Azure Active Directory Conditional Access * Deploy the Windows Defender ATP * Deploy the Azure Active Directory Identity Protection * Deploy the Azure Active Directory PIM * Deploy the Azure Active Directory Delegation of Admin design   Deploy one (1) Cloud PAW image on up to six (6) production workstations which are attached to Azure Active Directory, one (1) per in scope tenant   * Update test guide document. * Review test guide document with CUSTOMER NAME REMOVED. * Update implementation guide document. * Review implementation guide document with CUSTOMER NAME REMOVED. * Conduct functional testing using the test cases from the test guide. This activity is time-boxed to two (2) days. * Update the operations guide document. * Review the operations guide with CUSTOMER NAME REMOVED. |
| **CUSTOMER NAME REMOVED** **activities** The activities to be performed by CUSTOMER NAME REMOVED | * Participate in Build phase activities. * Participate in review activities. * Engage designated test users. * Perform system testing based on the test guide. * Review the operations guide and participate in its approval. |
| Key assumptions | * CUSTOMER NAME REMOVED SMEs will participate in the development sessions. * CUSTOMER NAME REMOVED will provide appropriate secure room facilities, including hardware and software. * CUSTOMER NAME REMOVED SMEs and test users are ready to participate in the testing activities. * A post-deployment support process will be established by CUSTOMER NAME REMOVED prior to commencement of the Deploy phase. * CUSTOMER NAME REMOVED will provide CUSTOMER NAME REMOVED-specific test cases. |

#### Enable

During the Enable phase, Microsoft will work with you to prepare, configure, and implement enable the Azure Cloud PAW solution for your production environment.

Table 67: PAW - Enable phase

|  |  |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | * Move Cloud PAW to the production environment   + - During Cloud PAW production implementation, Microsoft will assist as needed as CUSTOMER NAME REMOVED puts the implementation guide into effect.     - Microsoft support activities are limited to the first six (6) Cloud PAWs in the CUSTOMER NAME REMOVED production forest. * Handover and close out the project. |
| **CUSTOMER NAME REMOVED activities** The activities to be performed by CUSTOMER NAME REMOVED | * Deploy the solution to production. * Provide direction to Microsoft resources during this project phase. * Run CUSTOMER NAME REMOVED acceptance tests. * Provide feedback on production use. * Provide sign-off for project results. |
| Key assumptions | * CUSTOMER NAME REMOVED will take responsibility for its change control processes (e.g. submitting all necessary change requests). * Affected organisations will identify the resources and groups which will be required for the Deploy phase. |

## Deliverables

This section provides a list of the deliverables produced by the PAW project. If a deliverable requires formal review and acceptance (indicated by a Yes), it will be governed by the deliverable acceptance process as defined in section 2.5.

Table 68: PAW – Deliverables

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Phase** | **Deliverable name** | **Deliverable Description** | **Acceptance Required** | **Responsibility** |
| D28 | Assess | PAW Architecture and design document | Microsoft Word Document with Cloud PAW reference architecture including description of the solution and its components, logical solution and physical implementation. | Yes  Acceptance Criteria:  A Microsoft Word document of approximately 100 to 130 pages, that accurately describes the solution design | Microsoft |
| D29 | Assess | PAW Implementation guide document | A document with configuration information and step-by-step instructions used to build the end state described in the architecture and design document | No | Microsoft |
| D30 | Assess | PAW Test Guide | A document with test cases that documents testing procedures. | No | Microsoft |
| D31 | Remediate | PAW Operations guide document | A document with operational guidance for the systems and components which are described in the architecture and design document. | No | Microsoft |
| D32 | Enable | Up to four (4) production Cloud PAWs deployed | Up to four (4) production Cloud PAWs have been successfully deployed and tested. | No | Microsoft |

## Project roles and responsibilities

The key project roles and the responsibilities are as follows.

### CUSTOMER NAME REMOVED

Required CUSTOMER NAME REMOVED Roles are defined at the Program level in section 3.2.1.

### Microsoft

Table 69: PAW - Microsoft roles and responsibilities

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Responsibilities | Project Commitment | |
| PAW Consultant | * Provide technical design leadership * Deliver workshops and sessions * Responsible for development of technical deliverables | Full time |

### CUSTOMER NAME REMOVED responsibilities

Responsibilities include:

* A dedicated physically secure room with desks, chairs, and network access which the project team can use for the duration of the project (should be ready before the project kick off)
* A secure storage location for documentation and DVDs which will be used on the project (this place would preferably be in the secure room)
* At least one (1) DVD-writing device (external or built-in) in the project room
* A stack of 20 writable single-layer DVDs
* Paper shredder, ideally also capable of shredding DVD media
* A separate dedicated Internet connection for the secure room with at least 16 megabits a second downstream which can be used for the known-good media build process
* A centralised project repository for project information and documentation

Further to the above, CUSTOMER NAME REMOVED is to provide the following:

* At least one physical server used for the build and production environment capable of running virtual machines on Hyper-V.
* Four (4) unused and unopened laptops or desktops which will be used as production Cloud PAWs
* Test data and personnel which will be needed to conduct solution system testing, including interfaces.
* Test data and personnel which will be needed to conduct CUSTOMER NAME REMOVED acceptance testing of the solution, including interfaces.
* Log Analytics Contributor rights (Azure RBAC) on a Log Analytics workspace in one of CUSTOMER NAME REMOVED ’s Azure subscriptions for the user who will add the monitoring solutions to the Azure Log Analytics workspace. The Log Analytics workspace stores the log data, which are used to monitor Cloud PAWs.
* Access to Azure Active Directory, Azure Intune, Azure Conditional Access, Windows Defender ATP
* Log Analytics Reader rights (Azure RBAC) on a Log Analytics workspace in one of CUSTOMER NAME REMOVED ’s Azure subscriptions for the users who need to view and search Azure Log Analytics monitoring data.

# P06: Advanced Threat Detection Implementation Services (ATDIS)

## Objectives

In discussions between CUSTOMER NAME REMOVED and Microsoft It has been identified that detection of credential theft attempts is currently limited and is an area of critical importunate to a strong security posture.

CUSTOMER NAME REMOVED has a significant presence across Azure and Office 365 along with a significant fleet of end user and server systems. The use of the ATP security suite of detection tools allows CUSTOMER NAME REMOVED to have an early signal, backed by AI, to detect a breach attempt and move to a model that can operationalise incident response when it happens.

This project designs and implements:

* Azure Advanced Threat Protection | Advanced Threat Analytics
* Office 365 Advanced Threat Protection, and
* Windows Defender Advanced Threat Protection.

These components provide threat protection and detection services across multiple attack surfaces: Active Directory Domain Services, Azure virtual machines and web applications, Windows devices and Office 365 services.

* Provide an understanding of the threats that Windows Defender will block or mitigate.
* Provide an understanding of the threats for which Azure Advanced Threat Protection, Office 365 Advanced Threat Protection and Windows Defender Advanced Threat Protection will generate alerts.
* Assist with the creation of a response activation worksheet that is specific to the events that Azure Advanced Threat, and Windows Defender Advanced Threat Protection detect.
* Assist with the design and implementation of Azure Advanced Threat Protection to monitor for threats to CUSTOMER NAME REMOVED’s production Active Directory Domain Services (AD DS) environment.

## Areas in scope

### General project scope

The scope of this project is to help CUSTOMER NAME REMOVED prepare, design, and implement solutions using Azure Advanced Threat Protection, Office 365 Advanced Threat Protection and Windows Defender Advanced Threat Protection.

Microsoft will provide Services in support of the following scope:

Table 70: ATDIS – General project scope

|  |  |  |
| --- | --- | --- |
| Area | Description | Assumptions |
| Implement Azure Advanced Threat Protection for the CUSTOMER NAME REMOVED environment. | * Microsoft will help CUSTOMER NAME REMOVED implement Azure Advanced Threat Protection, deploy Azure Advanced Threat Protection Sensors, and configure Azure Advanced Threat Protection (including implementing syslog integration and configuring initial exclusions). * Microsoft will help CUSTOMER NAME REMOVED deploy Azure Advanced Threat Protection to detect threats in a production AD DS forest. Microsoft will also assist CUSTOMER NAME REMOVED with configuring one (1) Azure ATP workspace in one (1) Azure subscription for data collection and analysis. * This activity is time-boxed to 10 hours. | * If dedicated Azure ATP sensors are used, CUSTOMER NAME REMOVED personnel are responsible for configuring port mirroring for connectivity to the in-scope Azure ATP instance. * Up to two (2) AD DS forests * Up to one (1) Azure subscription * Up to one (1) Office 365 tenant. |
| Implement Windows Defender Advanced Threat Protection for the CUSTOMER NAME REMOVED environment. | * Microsoft will help CUSTOMER NAME REMOVED turn on Windows Defender Advanced Threat Protection for up to 10 supported Windows 10 client endpoints. * This activity is time-boxed to twenty-four (24) hours. | * CUSTOMER NAME REMOVED has implemented Windows Defender on the selected endpoints prior to the Remediation phase. * CUSTOMER NAME REMOVED will allow endpoints to communicate directly with the Windows Defender Advanced Threat Protection service endpoint. |
| Implement Office 365 Advanced Threat Protection for the Office 365 tenant. | * Microsoft will help CUSTOMER NAME REMOVED configure one (1) policy for each of the following policy options: * Antimalware * Anti-phishing * Antispam * Safe attachments * Safe links * This activity is time-boxed to twenty-four (24) hours. | * Microsoft will help CUSTOMER NAME REMOVED implement and configure Office 365 Advanced Threat Protection for a single Office 365 subscription. |
| Solution Tuning Assistance | * Microsoft will help CUSTOMER NAME REMOVED address any false positive detections in Azure Advanced Threat Protection, and Windows Defender Advanced Threat Protection that were identified during the Enable phase. * This assistance is limited to five (5) days. | CUSTOMER NAME REMOVED will assign operational staff that will work side by side with the Microsoft team to identify, review, follow up on, and address or remediate performance or detection problems as they occur. |

### Software products and technologies

The products and technology that are listed in the following table are required for the project. CUSTOMER NAME REMOVED is responsible for obtaining all identified licenses and products.

Table 71: ATDIS - Software products & technologies

|  |  |  |
| --- | --- | --- |
| Product and technology item | Version | Ready by |
| Azure Advanced Threat Protection | Not applicable | One week prior to the Enable phase |
| Azure subscription | Not applicable | One week prior to the Enable phase |
| Windows Defender Advanced Threat Protection | Not applicable | One week prior to the Enable phase |
| Office 365 subscription | Not applicable | One week prior to the Enable phase |
| Office 365 Advanced Threat Protection | Not applicable | One week prior to the Enable phase |
| Windows 10   * Windows Defender has been implemented | Build 1607 or newer | One week prior to the Enable phase |

### Environments

The following environments will be required to deliver the project.

Table 72: ATDIS - Environments

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Environment | AD DS forest name | Location | Responsibility | Ready by |
| Production | CUSTOMER NAME REMOVED AD DS forest | CUSTOMER NAME REMOVED | CUSTOMER NAME REMOVED | One week prior to the Enable phase |

### Testing

The following testing is included in the scope of the project. If CUSTOMER NAME REMOVED has responsibility for testing, the Microsoft effort to support that activity is identified. If additional time is needed for Microsoft testing support, then it can be requested through the change management process defined in the 2.7.3.

Table 73: ATDIS - Testing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test type (environment) | Description | Responsibility | | |
| Has responsibility  for testing? | Provides data or test cases | Provides guidance and support |
| System or functional testing (development) | System or functional testing focuses on determining whether functionality meets design. Test cases are based on the test plan document. The Microsoft effort to support this testing is limited to 8 hours**.** | Microsoft | CUSTOMER NAME REMOVED | CUSTOMER NAME REMOVED |

### Workshops

The following workshops will be delivered during the project.

Microsoft will require a dedicated room to deliver each of the workshops. The room configuration must include a projector, whiteboard and internet access.

Table 74: ATDIS - Workshops

|  |  |  |
| --- | --- | --- |
| Name | Description and location | Quantity and duration |
| Engagement kick-off | * The engagement kick-off meeting will cover the following topics:   + - Stakeholder introductions     - CUSTOMER NAME REMOVED project requirements and objectives     - An overview of Azure Advanced Threat Protection     - An overview of Windows Defender Advanced Threat Protection     - In scope or out of scope items     - Timeline and approach (overview)     - Project schedule review     - Roles and responsibilities     - Project communications     - Action items * Location: delivered onsite at the CUSTOMER NAME REMOVED facility in Sydney, Australia * Materials: Microsoft PowerPoint presentation * Project phase: Engagement initiation | * Number of sessions: 1 * Duration: up to 4 hours * Number of participants: up to 10 |
| Education workshop: understanding threats | * Description: this session provides a technical overview of common threats to modern IT organisations:   + - Viruses     - Malware     - Ransomware     - Credential theft     - Reconnaissance, persistence, and data exfiltration * Location: delivered onsite at the CUSTOMER NAME REMOVED facility in Sydney, Australia * Materials: PowerPoint presentation * Project phase: Assess | * Number of sessions: 1 * Duration: up to 8 hours * Number of participants: up to 10 |
| Education workshop: technical deep dive (Azure Advanced Threat Protection) | * Description: This session provides a technical deep dive into Azure Advanced Threat Protection   + - Azure Advanced Threat Protection architecture and components     - Detection mechanisms     - Requirements and prerequisites     - Configuration     - Integration * Location: delivered onsite at the CUSTOMER NAME REMOVED facility in Sydney, Australia * Materials: PowerPoint presentation * Project phase: Assess | * Number of sessions: 1 * Duration: up to 4 hours * Number of participants: up to 10 |
| Education workshop: technical deep dive (Windows Defender Advanced Threat Protection) | * Description: This session provides a technical deep dive into Windows Defender Advanced Threat Protection   + - Windows Defender Advanced Threat Protection architecture and components     - Detection, protection, and response mechanisms     - Requirements and prerequisites     - Configuration     - Integration * Location: delivered onsite at the CUSTOMER NAME REMOVED facility in Sydney, Australia. * Materials: PowerPoint presentation * Project phase: Assess | * Number of sessions: 1 * Duration: up to 4 hours * Number of participants: up to 10 |
| Education workshop: technical deep dive (Office 365 Advanced Threat Protection) | * Description: this session provides a technical deep dive into Office 365 Advanced Threat Protection   + - Office 365 Advanced Threat Protection architecture and components     - Detection, protection, and response mechanisms     - Requirements and prerequisites     - Configuration     - Integration * Location: delivered onsite at the CUSTOMER NAME REMOVED facility in Sydney. * Materials: PowerPoint presentation * Project phase: Assess | * Number of sessions: 1 * Duration: up to 4 hours * Number of participants: up to 10 |
| Solution enablement workshop: design decisions (Azure Advanced Threat Protection) | * Description: Microsoft will lead up a design decision workshop focusing on Azure Advanced Threat Protection which will be used to determine the specific design (or designs) required to achieve CUSTOMER NAME REMOVED’s goals. * Design decisions include, but are not limited to:   + - Assessment of Azure Advanced Threat Protection sensor installation on domain controllers     - Hardware selection for, and placement of, Azure Advanced Threat Protection standalone sensors     - Selection of domain controllers to assess during limited scope implementation     - Configuration options within Azure Advanced Threat Protection     - Assignment of roles and access within Azure Advanced Threat Protection * Location: delivered onsite at the CUSTOMER NAME REMOVED facility in Sydney, Australia * Materials: PowerPoint presentation * Project phase: Assess | * Number of sessions: 1 * Duration: up to 4 hours * Number of participants: up to 10 |
| Solution enablement workshop: design decisions (Windows Defender Advanced Threat Protection) | * Description: Microsoft will lead a design decision workshop that is focused on Windows Defender Advanced Threat Protection and that will be used to determine the specific design or designs required to achieve CUSTOMER NAME REMOVED’s goals. * Design decisions include, but are not limited to:   + - Selection of in-scope endpoints for Windows Defender Advanced Threat Protection implementation     - Integration of Windows Defender Advanced Threat Protection and Azure Advanced Threat Protection workspaces (if applicable)     - Integration of Windows Defender Advanced Threat Protection and Office 365 Advanced Threat Protection (if applicable) * Location: delivered onsite at the CUSTOMER NAME REMOVED facility in Sydney, Australia * Materials: PowerPoint presentation * Project phase: Assess | * Number of sessions: 1 * Duration: up to 4 hours * Number of participants: up to 10 |
| Solution enablement workshop: design decisions (Office 365 Advanced Threat Protection) | * Description: Microsoft will lead a design decision workshop that is focused on Office 365 Advanced Threat Protection and that will be used to determine the specific design or designs required to achieve CUSTOMER NAME REMOVED’s goals. * Design decisions include, but are not limited to:   + - Determination of which features to implement for Office 365 Advanced Threat Protection, and for which Office 365 components     - Design of policies for anti-phishing, safe attachments, anti-spam, anti-malware, and safe links     - Assignment of roles and access within Office 365 Advanced Threat Protection * Location: delivered onsite at the CUSTOMER NAME REMOVED facility in Sydney. * Materials: PowerPoint presentation * Project phase: Assess | * Number of sessions: 1 * Duration: up to 4 hours * Number of participants: up to 10 |
| Remediation planning workshop | * Description: the goal of this session is to identify problems in CUSTOMER NAME REMOVED’s environment that must be resolved before implementation of the in-scope solution. Once problems have been identified, the team will determine appropriate steps for remediation or mitigation and assigned owners to complete those steps. * Location: delivered onsite at the CUSTOMER NAME REMOVED facility in Sydney, Australia * Materials: PowerPoint presentation * Project phase: Assess | * Number of sessions: 1 * Duration: up to 2 hours * Number of participants: up to 10 |
| Education workshop: operational excellence | * Description: this session focuses on the operational elements of managing the components in the in-scope solution components. Topics include:   + - General usage     - Configuration options     - Backup and restore     - Troubleshooting * Location: delivered onsite at the CUSTOMER NAME REMOVED facility in Sydney, Australia. * Materials: PowerPoint presentation * Project phase: Enable | * Number of sessions: Up to 4 * Duration: up to 4 hours * Number of participants: up to 10 |
| Test workshop: review the test specification with CUSTOMER NAME REMOVED | * Description: this session focuses on the test specification that will be used to validate the in-scope components of the solution.   + - Describe testing methodology     - Review default test specification     - Identify CUSTOMER NAME REMOVED specific scenarios     - Collect feedback from CUSTOMER NAME REMOVED on required changes * Location: delivered onsite at the CUSTOMER NAME REMOVED facility in Sydney, Australia. * Materials: Microsoft Word document * Project phase: Enable | * Number of sessions: 1 * Duration: up to 2 hours * Number of participants: up to 10 |
| Security incident response workshop: suspicious activity classifications and response process definition (Azure Advanced Threat Protection.) | * Description: this session focuses on the immediate response to suspicious activities detected by Azure Advanced Threat Protection.   + - Triaging suspicious activity     - Defining, scoping, and assessing suspicious activity     - Classifying suspicious activity     - Preparing for a major incident     - Declaring a breach * Location: delivered onsite at the CUSTOMER NAME REMOVED facility in Sydney, Australia * Materials: PowerPoint presentation * Project phase: Enable | * Number of sessions: 1 * Duration: up to 2 hours * Number of participants: up to 10 |
| Security incident response workshop: security incident classifications and response process definition (Windows Defender Advanced Threat Protection) | * Description: this session focuses on the immediate response to security incidents detected by Windows Defender Advanced Threat Protection.   + - Triaging a security incident     - Defining, scoping, and assessing a security incident     - Classifying security incident     - Preparing for a major incident     - Declaring a breach * Location: delivered onsite at the CUSTOMER NAME REMOVED facility in Sydney, Australia. * Materials: PowerPoint presentation * Project phase: Enable | * Number of sessions: 1 * Duration: up to 2 hours * Number of participants: up to 10 |
| Security incident response workshop: communication process discussion | * Description: this session continues the security incident response conversation and focuses on the critical communications-related activities that accompany an incident.   + - Identify owners of the communications process     - Define the audiences and messages     - Identify the information that needs to be disseminated     - Identify the channels to be used for communications     - Define the criteria for breach declaration and define the ownership of that declaration * Location: delivered onsite at the CUSTOMER NAME REMOVED facility in Sydney, Australia. * Materials: PowerPoint presentation * Project phase: Enable | * Number of sessions: 1 * Duration: up to 4 hours * Number of participants: up to 10 |
| Security incident response workshop: security response tabletop exercise | * Description: Microsoft will lead a table top exercise during which CUSTOMER NAME REMOVED personnel will simulate their response to a security alert generated by the threat detection solution. This exercise will help solidify understanding of the core concepts discussed in the other security incident response workshops and enhance the ability of CUSTOMER NAME REMOVED personnel to identify and respond to incidents. * Location: delivered onsite at the CUSTOMER NAME REMOVED facility in Sydney, Australia. * Materials: PowerPoint presentation * Project phase: Enable | * Number of sessions: 1 * Duration: up to 4 hours * Number of participants: up to 10 |

## Areas out of scope

Any area not explicitly included in the areas in scope section, is out of scope for Microsoft during this project. Areas out of scope for this project are listed in the following table.

Table 75: ATDIS - Out of scope

|  |  |  |
| --- | --- | --- |
| Area | Description | |
| Azure Advanced Threat Protection activation | The following are not included:   * Configuration of port mirroring for environments that require Azure Advanced Threat Protection standalone sensors * Any integration of SIEM events into Azure Advanced Threat Protection. * Configuration of threat detection for more than two (2) AD DS forests * Configuration of multiple Azure Advanced Threat Protection workspaces   Azure ATP relies on analysing multiple network protocols, as well as events collected from the SIEM or via Windows Event Forwarding. Detections based on network protocols with encrypted traffic (for example, LDAPS and IPSEC) are not analysed. Domain controllers which uses encrypted traffic is out of scope for this project. |
| Windows Defender Advanced Threat Protection | The following are not included:   * Implementation of Windows Defender Advanced Threat Protection for unsupported clients * SIEM integration |

## Project approach

### Approach

This project follows the Online Services Lifecycle methodology, and work is divided into 3 distinct phases: Assess, Remediate, and Enable. Each phase has distinct activities which are described in the following sections.



Figure 11: ATDIS - Approach

### Assess

During the Assess phase, Microsoft will work with you to begin the project and complete the design and planning workshops. The result is a modern threat detection design that will be built, deployed, and configured into your production environment during the Enable phase.

Table 76: ATDIS - Assess phase

|  |  |  |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | * Conduct the project kick-off session. This session covers the overall project scope, structure of involved team members, the approach that will be used to complete the project, and the timeline for overall completion. In addition, Microsoft will present an overview of the in-scope solution components:   + - Azure Advanced Threat Protection     - Windows Defender Advanced Threat Protection     - Office 365 Advanced Threat Protection * Conduct the technical education workshops.   + - Understanding threats—this session provides a technical overview of common threats to modern IT organisations.     - Technical deep dives—these sessions provide technical deep dives into the in-scope solution components: * Azure Advanced Threat Protection * Windows Defender Advanced Threat Protection * Office 365 Advanced Threat Protection * Conduct the solution enablement workshops. During these sessions, Microsoft will work with you to identify critical design decisions that will in turn be used to develop an appropriate design for your threat detection solution components:   + - Azure Advanced Threat Protection     - Windows Defender Advanced Threat Protection     - Office 365 Advanced Threat Protection * Conduct the remediation planning workshop. During this session, Microsoft will work with you to identify problems in the environment that must be resolved or mitigated to promote the success of the threat detection solution project. * Document the solution enablement plan. Microsoft will include project requirements and solution design strategies in the solution enablement plan that are derived from the solution enablement activation workshop. * Document the remediation checklist. Microsoft will document the problems that must be remediated during the Remediate phase. |
| **CUSTOMER NAME REMOVED** **activities** The activities to be performed by CUSTOMER NAME REMOVED | * Work with Microsoft to identify project team members. * Identify and schedule rooms for meetings and educational workshops. * Facilitate any necessary communication or information in preparation for requests that might result from discussions during the Envision workshop, including information-gathering exercises. * Identify staff members who will participate in appropriate educational workshops based on their roles and responsibilities within the organisation. * Identify staff members who will participate in the solution enablement workshop based on their roles and responsibilities within the organisation. * Participate in the review and approval process of the solution enablement plan document and remediation checklist deliverables. |
| Key assumptions | * CUSTOMER NAME REMOVED will schedule and coordinate appropriate personnel to attend the project kick-off meeting. * CUSTOMER NAME REMOVED will coordinate appropriate resources for each educational module and will schedule meeting rooms to accommodate the size of the group. * CUSTOMER NAME REMOVED will coordinate appropriate resources for the solution enablement workshops and will schedule meeting rooms to accommodate the size of the group. * CUSTOMER NAME REMOVED will participate in the review and approval of the solution enable plan and remediation checklist. |

### Remediate

During the Remediate phase, the team will resolve or mitigate all items in the remediation checklist that was developed during the remediation planning workshop in the Assess phase.

Table 77: ATDIS - Remediate phase

|  |  |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | * Provide CUSTOMER NAME REMOVED up to 5 days of remediation activity assistance. * Update and finalise the remediation checklist based on CUSTOMER NAME REMOVED’s feedback. |
| **CUSTOMER NAME REMOVED** **activities** The activities to be performed by CUSTOMER NAME REMOVED | * Perform the remediation activities, resolving or mitigating all items in the remediation checklist. * Provide feedback to Microsoft related to the solution enablement plan and remediation checklist. |
| Key assumptions | * CUSTOMER NAME REMOVED is responsible for all remediation activities and will perform them with Microsoft assistance. Microsoft is not responsible for any remediation activities. * CUSTOMER NAME REMOVED will communicate the actions taken and the results of those actions to Microsoft for inclusion in the updated remediation checklist and solution enablement plan. |

### Enable

During the Enable phase, Microsoft will work with you to prepare, configure, and implement enable the threat detection solution for your production network environment.

Table 78: ATDIS - Enable phase

|  |  |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | * Conduct the operational excellence educational workshops. * Conduct the test workshop to review the test specification with CUSTOMER NAME REMOVED . * Update the test specification based on CUSTOMER NAME REMOVED feedback. * Assist with the configuration of the required Azure workspace for Azure Advanced Threat Protection. Microsoft will provide up to 2 hours of assistance in support of this component of the in-scope solution. * Assist with the configuration of Azure Advanced Threat Protection sensors on domain controllers or the configuration of Azure Advanced Threat Protection standalone sensors. Microsoft will provide up to 8 hours of assistance in support of this component of the in-scope solution. * Assist with the configuration of 1 security policy for 1 Azure subscription within Azure Security Center. * Assist with the implementation of Office 365 Advanced Threat Protection and of in-scope policies. Microsoft will provide up to 8 hours of assistance in support of this component of the in-scope solution. * Assist with the implementation of Windows Defender Advanced Threat Protection for up to 10 supported Windows 10 endpoints. Microsoft will provide up to 8 hours of assistance in support of this component of the in-scope solution. * Assist with the functional testing of the deployed solution. * Provide P1 defect remediation. * Review suspicious activities with CUSTOMER NAME REMOVED and provide guidance related to tuning and configuring exclusions. Microsoft will provide up to 5 days of assistance in support of this component of the in-scope solution. * Conduct the security incident response preparation workshops. * Document the security incident response classification worksheet and review it with CUSTOMER NAME REMOVED . * Update the security incident response worksheet based on CUSTOMER NAME REMOVED feedback. * Prepare the closeout meeting. Microsoft will validate the completion of deliverables and prepare a closeout meeting to recap the project. * Participate in the closeout meeting. Microsoft will lead a closeout meeting that will include reviewing the configuration and implementation of the in-scope solution and finalising the completion of deliverables. |
| **CUSTOMER NAME REMOVED activities** The activities to be performed by CUSTOMER NAME REMOVED | * Help make sure that personnel attend workshops during this phase. * Schedule meeting rooms for each workshop session. * Participate in the review and approval of the test specification. * Coordinate, submit, and approve the change management requests required to deploy the in-scope solution components into the production environment. * Coordinate the procurement and installation of systems that were identified as necessary in the solution design document and are required for the Enable phase. The Enable phase includes default operating system configuration and supporting operational software in addition to Azure Advanced Threat Protection * Configure the required Azure workspace for Azure Advanced Threat Protection. * Configure network port mirroring between the AD DS domain controllers (source) and the Azure Advanced Threat Protection standalone sensor systems (destination) for systems not using the Azure Advanced Threat Protection sensor * Install and configure Windows systems that support Azure Advanced Threat Protection implementation as documented in the solution enablement plan. * Implementation of Office 365 Advanced Threat Protection and configuration of in-scope policies. * Implementation of Windows Defender Advanced Threat Protection and configuration of the in-scope endpoints. * Validation of communication between in-scope endpoints and the Windows Defender Advanced Threat Protection service endpoint * Provision operational staff who are responsible for managing and monitoring events captured by Azure Advanced Threat Protection and Windows Defender Advanced Threat Protection, who will help the Microsoft team review those events, and who will make configuration adjustments as needed to reduce the identification of benign positives. * Manage all required change management requests and approvals for the implementation of the in-scope solutions. * Perform functional testing based on the test specification. * Review the security incident response classifications worksheet and provide feedback to Microsoft. * Submit change requests for the implementation of systems that are required for the in-scope solution as defined in the solution design document. * Coordinate the personnel who are needed to help install and configure the in-scope threat detection solution components. * Schedule and coordinate the attendance of required personnel to attend the project closeout meeting. |
| Key assumptions | * CUSTOMER NAME REMOVED will have obtained all required host systems (physical or virtual) that will be used for production implementation and they will be available by the start of this phase so that validation activities can be performed. * CUSTOMER NAME REMOVED will coordinate and communicate the contents of the security incident response classifications worksheet within its organisation. * The security incident response classifications worksheet is not intended to be a complete organisational incident response plan but will be used by CUSTOMER NAME REMOVED as a resource for responding to events discovered by Azure Advanced Threat Protection and Windows Defender Advanced Threat Protection or it might be integrated into a broader incident response plan. * CUSTOMER NAME REMOVED will use the design that is documented in the solution design document to procure the appropriate resources (such as hardware or virtual machines) that are required to deploy Azure Advanced Threat during the Enable phase. If network port mirroring is required to support the implementation of Azure Advanced Threat, CUSTOMER NAME REMOVED will coordinate appropriate network personnel to document and configure it for the solution. * Azure Advanced Threat Protection will be deployed on a production network. It will monitor production domain controllers. * CUSTOMER NAME REMOVED will use the Azure Advanced Threat Protection sensor for their Azure Advanced Threat Protection activation. If not using the Azure Advanced Threat Protection Sensor, CUSTOMER NAME REMOVED will configure port mirroring between in-scope AD DS domain controllers (source) and Azure Advanced Threat Protection standalone sensor systems (destinations) in support of the in-scope solution. * The Azure Advanced Threat Protection standalone sensor systems will be installed in an isolated workgroup that is non–domain joined. * When Azure Advanced Threat Protection is first installed, it might find problems in the environment. CUSTOMER NAME REMOVED will provide personnel who can help determine whether the recorded event is a benign positive or the indication of an actual attack. If it is a benign positive, CUSTOMER NAME REMOVED will work with Microsoft to make configuration adjustments designed to address the benign positive event. * Test cases other than those that have been listed as in scope will be completed by CUSTOMER NAME REMOVED and will not affect the completion of this project. * Required configuration changes will be made within the time frame that has been identified for tuning assistance. |

## Deliverables

This section provides a list of the deliverables produced by the ATDIS project. If a deliverable requires formal review and acceptance (indicated by a Yes), it will be governed by the deliverable acceptance process as defined in section 2.5.

Table 79: ATDIS – Deliverables

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Phase | Deliverable name | Deliverable Description | Acceptance Required | Responsibility |
| D33 | Assess | ATDIS Solution enablement plan | The solution enablement plan documents the technical design of the solution and includes all important design decisions. | Yes.  Acceptance Criteria:  CUSTOMER NAME REMOVED agrees that the document is an appropriate reflection of its desired design, and that it includes all important design decisions. | Microsoft |
| D34 | Assess | ATDIS Remediation checklist | The remediation checklist identifies all tasks and problems in the CUSTOMER NAME REMOVED environment that must be remediated before the solution is built, deployed, and configured in the Enable phase. | Yes.  Acceptance Criteria:  CUSTOMER NAME REMOVED agrees that the list includes all required remediation items. | Microsoft |
| D35 | Enable | ATDIS Test specification | A document that details the steps needed to validate the in-scope components of the solution | Yes.  Acceptance Criteria:  CUSTOMER NAME REMOVED agrees that the test specification meets its objectives for validating the solution functionality for production implementation. | Microsoft |
| D36 | Enable | ATDIS Security incident response classifications worksheet | A worksheet that includes the complete list of potential detections and default classifications, and which will be revised to include the updated risk classifications unique to CUSTOMER NAME REMOVED | Yes.  Acceptance Criteria:  CUSTOMER NAME REMOVED agrees that the worksheet reflects the revised risk classifications based on CUSTOMER NAME REMOVED’s environment. | Microsoft |

## Project roles and responsibilities

The key project roles and the responsibilities are as follows:

### CUSTOMER NAME REMOVED

Required CUSTOMER NAME REMOVED Roles are defined at the Program level in section 3.2.1.

### Microsoft

Table 80: ATDIS - Microsoft roles and responsibilities

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Responsibilities | Project Commitment | |
| ATDIS Consultant | * Provide technical design leadership. * Deliver workshops and sessions. * Responsible for development of technical deliverables. | Full time |

# P07: Modern Desktop Deployment (MDD)

## Objectives

This project focuses on gaining control of the privileged accounts that manage the System Center deployment platform for Windows end user computing (which often include administrator systems). This project assumes the current platform is untrusted and builds the base system from known good media and a trusted keyboard.

Using the Microsoft System Center Configuration Manager (SCCM) deployment methodology and approach, Microsoft Services will deliver System Center Configuration Manager deployment to support the rollout of a secure Windows 10 Desktop.

The objective of this project is to:

* Provide planning and technical solution design using System Centre Configuration Manager;
* Install and configure System Centre Configuration Manager site into production; and to
* Provide initial testing of the deployment and image for Windows 10.

## Areas in scope

### General project scope

The primary objective of this project is to provide CUSTOMER NAME REMOVED with a SCCM environments with newly built Windows 10 current branch image.

Microsoft will provide Services in support of the following scope:

Table 81: MDD – General project scope

|  |  |  |
| --- | --- | --- |
| Area | Description | Assumptions |
| Workshops | * Microsoft will deliver up to two (2) 3-hour workshops to gather and document the design requirements for the SCCM environments. * Deliver one (1) additional full-day workshop to gather and document the design requirements for the Windows 10 Current Branch. * Deliver 3 (one) 1-hour workshops for Windows Servicing | * CUSTOMER NAME REMOVED will make available the staff members required to participate in the educational workshops. * CUSTOMER NAME REMOVED will provide the facilities (room, whiteboard & projector) required for conducting the workshops. * CUSTOMER NAME REMOVED will provide access to any existing SCCM build and design documentation. |
| Core SCCM Infrastructure | * The planning and design of the following Configuration Manager infrastructure that is used for on-premises:   + - 1 primary site     - Up to five (5) distribution points     - 1 reporting point * Role-based access administration * Implement 1 client setting for hardware and software inventory, remote control, power management, and health attestation. | CUSTOMER NAME REMOVED will provide the infrastructure and servers for the implementation of SCCM |
| Windows Servicing | * Configure Windows 10 features and quality update management with Configuration Manager * Design and implement up to four (4) servicing plans for managing Windows 10 semi-annual feature updates. * Design and implement two (2) automatic deployment rules for managing Windows 10 quality Updates | - |
| Windows Image | * Create the following Windows 10 Enterprise reference image using a single image design and the image factory:   + - 1 64-bit image (default)     - 1 32-bit image (only if required)     - Inclusion of up to 5 applications in the image     - Configuration of up to 10 custom image settings * Installation of all publicly released and recommended updates through WSUS or Windows Update when the image is created * Implement additional plug-and-play device driver support for up to five (5) makes and models of devices in Configuration Manager. | * CUSTOMER NAME REMOVED will provide up to five (5) applications. Additional applications can be added via a Change Request. * Application remediation is out of scope for this project. |
| Windows Deployment | * Design and implement a single Configuration Manager operating system deployment task sequence for a new computer or refresh deployment. * Deploy new Image to up to five (5) devices for testing * Provide guidance pertaining to BIOS-to-Unified Extensible Firmware Interface–conversion (MBR2GPT.exe) as part of the deployment. * Implement plug-and-play device driver support for up to five (5) makes and models of devices (if not available). | * CUSTOMER NAME REMOVED will provide up to 5 (five) Windows 10 UEFI devices that support TPM 2.0 or greater. |
| Security Foundations | * Create a GPO that is based on the Windows 10 security baseline which include the following features:   + - BitLocker     - Credential Guard     - Application Guard     - Exploit Guard     - User Account Control     - Windows Defender Antivirus     - Windows Defender SmartScreen     - Dynamic Lock | - |

### Software products and technologies

The products and technology that are listed in the following table are required for project execution. CUSTOMER NAME REMOVED is responsible for obtaining all identified licenses and products.

Table 82: MDD - Software products and technologies

|  |  |
| --- | --- |
| Product and technology item | Ready by |
| Windows 10 Enterprise Edition (latest version) | Two weeks prior to commencing the project |
| Windows Server 2012 R2 Standard (or later) for SCCM infrastructure (physical or virtual machines) | Two weeks prior to commencing the project |
| Microsoft SQL Server 2014 Standard or Enterprise Edition (Latest version) | Two weeks prior to commencing the project |
| System Centre Configuration Manager Current Branch | Two weeks prior to commencing the project |
| All CUSTOMER NAME REMOVED software to be deployed as part of the project (limited to up to 5 applications) | Two weeks prior to commencing the project |

### Environments

The following environments will be required to deliver this project

Table 83: MDD - Environments required

|  |  |  |  |
| --- | --- | --- | --- |
| Environment | Location | Responsibility | Ready by |
| Production | CUSTOMER NAME REMOVED Datacentre | CUSTOMER NAME REMOVED | Start of the project |

### Testing

The following testing is included in the scope of the project. If CUSTOMER NAME REMOVED has responsibility for testing, the Microsoft effort to support that activity is identified. If additional time is needed for Microsoft testing support, then it can be requested through the change management process described in this SOW.

Table 84: MDD - Testing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test type (environment) | Description | Responsibility | | |
| Has responsibility  for testing? | Provides data or test cases | Provides guidance and support |
| System testing (SCCM Production environment) | Functionality testing focuses on determining whether functionality meets design. Test cases will be based on the technical guide document. (timeboxed to one (1) day of effort) | Microsoft | Microsoft | CUSTOMER NAME REMOVED |
| Image UAT testing (in production) | Microsoft will test the deployment of the Windows 10 image onto devices provided by CUSTOMER NAME REMOVED (timeboxed to two (2) days of effort) | Microsoft | Microsoft | CUSTOMER NAME REMOVED |

## Areas out of scope

Any area not explicitly included in the areas in scope section is out of scope for Microsoft during this project. Areas out of scope for this project, in addition to those listed elsewhere in this document, are listed in the following table.

Table 85: MDD - Out of scope

|  |  |  |
| --- | --- | --- |
| Area | Description | |
| All | * Design and implementation of a new Windows KMS infrastructure * Operating system upgrades of KMS servers, domain controllers, WSUS servers, or MDOP servers * Unsupported KMS servers * Creation of an Active Directory Domain Services (AD DS) group policy central store * Assessment, review, and modification of existing group policies * Design and implementation of a new servicing infrastructure using WSUS * Network and firewall configuration |
| Windows Servicing | * Third-party software update management * Feature update testing or quality update testing * Support for additional Microsoft products in Configuration Manager software update management * Windows Autopilot * Configuration and deployment of windows Analytics * Application portfolio discovery and rationalisation * Remediation of the existing environment and infrastructure. |
| Windows Image | * Evaluation of the image for regulatory compliance * Recommended practices that address compliance requirements * Identification of silent installation commands or creation of unattended installation scripts for application installers * Creation of scripts for automating image-setting customisation or configuration |
| Windows Deployment | * New device firmware preparation and configuration * Device driver remediation * Any existing hardware modification * Custom configuration XML files for the USMT * Any application compatibility testing or remediation * Identification of silent installation commands or the creation of unattended installation scripts for application installers * Creation of scripts for automating operating system settings, customisation, and configuration * Logistic and resource planning and allocation for deployment and migration activities |
| Security Foundations | * Design or implementation of security capabilities that are not listed in scope such as:   + - Windows Defender Advanced Threat Protection     - Windows Information Protection     - Device Guard     - Windows Hello for Business * Assessment, review, or modification of existing group policies * Creation of an AD DS group policy central store * Installation of new ADMX templates |

## Approach

The project will be structured following the Microsoft Online Services Lifecycle (OSL) methodology across three of the possible four distinct phases: Assess, Remediate and Enable. Each phase has distinct activities that are described in the following sections.

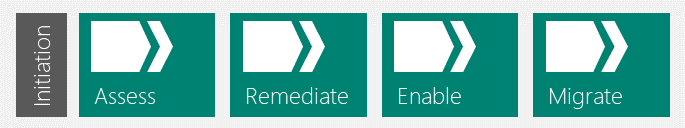


Figure 12: MDD - Approach

### Assess

During the Assess phase, Microsoft will conduct a series of workshops to gather design requirements. Microsoft, and CUSTOMER NAME REMOVED will review the results of the planning workshops and jointly determine requirements necessary to support the deployments.

Table 86: MDD - Assess phase

|  |  |  |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | **General activities**   * Conduct up to two (2) 3-hour decision-making workshops for each of the following services to gather requirements:   + - Design & implement System Center     - Configuration Manager core infrastructure     - Design and pilot new or refresh deployment     - Design and implement Windows servicing     - Security foundations   **Infrastructure foundations**   * Assess and validate the existing infrastructure:   + - Activation (Windows KMS)     - ADMX templates     - WSUS     - MDOP solution   **Windows 10 Current Branch**   * Conduct a full-day workshop to gather and document the design requirements for the Windows 10 Current Branch.   **Design and implement the servicing process**   * Workshop delivery: present up to three (3) workshops to CUSTOMER NAME REMOVED that can help define an approach to stay current with Windows as a Service. The workshops will include the following topics:   + - Compatibility     - Deployment (infrastructure, configuration, and operations)     - Capability and modernisation |
| **CUSTOMER NAME REMOVED** **activities** The activities to be performed by CUSTOMER NAME REMOVED | * Provide access to key personnel, service-level agreements, the current environment, and documentation. * Participate in workshops: provide detailed insights on application portfolio, infrastructure, configuration, and operational processes during design workshops to verify that appropriate guidance can be provided in the design document and implementation guide. * Plan and identify up to five (5) target devices or users for the deployment. * Prepare hardware client devices. * Prepare applications to be installed as part of the deployment. * Prepare test client devices. * Prepare device drivers. * Prepare the production environment infrastructure. |
| Key assumptions | * All required CUSTOMER NAME REMOVED personnel will attend workshops. * Decisions will be made during the workshops, by CUSTOMER NAME REMOVED to complete the final deployment and configuration process. * The network infrastructure is healthy. * CUSTOMER NAME REMOVED is aware of the existing corporate patching process and policies. * CUSTOMER NAME REMOVED is aware of the existing corporate standard image requirements and policies. * The latest System Center Configuration Manager Current Branch version will be installed. * CUSTOMER NAME REMOVED will perform necessary network and infrastructure changes to support the deployment. |

### Remediate

The remediate phase is not required for this project as the SCCM environment and Windows 10 image will be built as new without legacy environments, migration or existing data.

### Enable

The Enable phase includes the production implementation of the solution and the initial 5 device deployment (to test the image). The 5-device pilot deployment will be deemed successful if each technical component passes the functional test criteria and test cases defined in the technical guide that was developed as part of the project.

Table 87: MDD - Enable phase

|  |  |  |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | **Design and implement Configuration Manager core infrastructure**   * Build the production Configuration Manager infrastructure and configure the environment; such activities include:   + - The configuration of one (1) client setting     - Role-based access administration configuration   **Design and implement Windows servicing**   * Configure the following in the production environment and validate that they are working as designed:   + - Feature updates (either one): * Servicing plans for Windows 10 * GPOs   + - Quality updates (either one): * Automatic deployment rules * GPOs   **Windows Image**   * Create the following Windows 10 Enterprise reference image using a single image design:   + - One 64-bit image (default)     - One 32-bit image (only if required)     - Inclusion of up to five (5) applications in the image     - Configuration of up to ten (10) custom image settings * Install all publicly released and recommended updates through WSUS or Windows Update when creating the image. * Import drivers for up to five (5) hardware makes and models. * Validate that the drivers can be installed from Configuration Manager.   **Windows Deployment**   * Implement the deployment task sequence in production and validate that it is working. * Import drivers for up to five (5) hardware makes and models. * Perform an alpha deployment on up to five (5) desktop devices and support resolution of deployment problems within five (5) working days. * Conduct a go-or-no-go meeting to review problems and resolutions related to deployment readiness.   **Security foundations**   * Configure the GPO in the production environment and validate that the settings are applied to the devices. |
| **CUSTOMER NAME REMOVED** **activities** The activities to be performed by CUSTOMER NAME REMOVED | * Update the following production infrastructure and validate that the update has successfully completed:   + - Activation (Windows KMS)     - Administrative templates (ADMX) templates     - WSUS * Supply all hardware, virtual machines, operating systems built, and software required for the deployment of SCCM * Prepare the infrastructure for the Configuration Manager environment. * If necessary, verify the configuration of the network firewall, routers, and switches to permit standard client-to-server and server-to-server communication. * Infrastructure remediation—install, upgrade, or configure infrastructure configuration support services such as AD DS. * Remedy network services as required. * Remedy server problems as required. * Begin production backup and restore operations. * Assign a point of contact for each facility that has users who will be migrated. * Provide first-level and second-level support.   **Design and implement Windows servicing**   * Validate that the settings have been configured correctly and as designed.   **Windows Image**   * Provide all required software and licenses. * Provide the script or scripts needed to perform image-setting customisations. * Validate that the image created conforms to the design. * Validate that the image is functional. * Provide Windows 10 supported drivers for each hardware make and model   **Windows Deployment**   * Provide a list of target devices or users for the deployment. * Provide hardware client devices. * Provide and import applications (up to 5) to be installed as part of the deployment in Configuration Manager. * Import applications into Configuration Manager. * Provide the corporate standard Windows 10 image. * Communicate with users targeted for deployment. * Conduct user training and maintain communication with pilot users. * Provide first-level help desk support. * Provide desk-side support.   **Security foundations**   * Validate that the policies have been applied correctly and do not conflict with existing policies. |

## Deliverables

This section provides a list of the deliverables produced by the MDD project. If a deliverable requires formal review and acceptance (indicated by a Yes), it will be governed by the deliverable acceptance process as defined in section 2.5.

Table 88: MDD – Deliverables

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Phase** | **Deliverable name** | **Deliverable Description** | **Acceptance Required** | **Responsibility** |
| D37 | Assess | MDD Solution design document | Microsoft Word document that contains a description of the technical functionalities of the solution. | Yes  Acceptance Criteria:  A Microsoft Word document of approximately 100 to 130 pages, that accurately describes the solution design | Microsoft |
| D38 | Assess | MDD Preliminary test plan | Microsoft Word document that describes the strategy and approach that was used to plan, organise and manage the project’s testing activities. It identifies testing objectives, methodologies and tools, expected results, responsibilities and resource requirements.  The test plan details functional test cases for the solution and is provided in a preliminary format until the test cases have been completed and documented. | No | Microsoft |
| D39 | Assess | MDD Environment Information and Details | Details on the environment as well as infrastructure details for Microsoft to deploy SCCM | No | CUSTOMER NAME REMOVED |
| D40 | Enable | MDD Final Solution design document | Microsoft Word document that contains a description of the technical functionalities of the solution. | Yes  Acceptance Criteria:  A Microsoft Word document of approximately 100 to 130 pages, that accurately describes the solution design | Microsoft |
| D41 | Enable | MDD Final Test Plan | Microsoft Word document that describes the strategy and approach that was used to plan, organise and manage the project’s testing activities. It identifies testing objectives, methodologies and tools, expected results, responsibilities and resource requirements.  The test plan details functional test cases for the solution and is provided in a preliminary format until the test cases have been completed and documented. | Yes  Acceptance Criteria:  A Microsoft Word document of approximately 25 – 40 pages, that includes the expected test results and notes about implementing the defined test cases. | Microsoft |
| D42 | Enable | Up to five (5) desktops | Up to five (5) production desktops have been successfully deployed and tested | No | Microsoft |

## Project roles and responsibilities

The key project roles and the responsibilities are as follows.

### CUSTOMER NAME REMOVED

Required CUSTOMER NAME REMOVED Roles are defined at the Program level in section 3.2.1.

### Microsoft

Table 89: MDD - Microsoft roles and responsibilities

|  |  |
| --- | --- |
| Role | Responsibilities |
| Modern Desktop Consultant | * Participate in design and technical workshops. * Responsible for building the environment components and the required for the project. * Responsible for the 5-device pilot deployment. |

# P08: Modern Server Deployment (MSD)

## Objectives

Building on the P07 - Modern Desktop Deployment project, this project focuses on gaining control of the privileged accounts that manage the System Center deployment platform for Windows Server deployments. This is critical as most organisations will leverage a hypervisor platform and will have “golden images” that are copied over and over each time a server workload is required to be built. Leveraging a clean deployment platform protects the source image from being corrupted by and APT and allows a trusted server image to be deployed repeatedly.

This project assumes the current platform is untrusted and builds the base system from known good media and a trusted keyboard:

* Design and deploy a distinct System Center Configuration Manager (SCCM) deployment infrastructure for Windows Server 2019
* Implement a secured Tier 1 Role Based Access and Control (RBAC) model for roles that require the permission to “create” or “edit” an automation sequence or any privileged administrative function of the SCCM infrastructure
* Implement a secured and isolated Tier 2 Role Based Access and Control (RBAC) model for roles that require the permission to “execute” an automation sequence for OS deployment
* Implement the following security functionality into the Windows Server 2019 OS:
  + Security Baseline: application of the baseline security controls to the devices based on the Microsoft Security Compliance Manager, Enhanced Mitigation Experience Toolkit (EMET) controls and the Australian ISM Manual

## Areas in scope

### General project scope

The primary objective of this project is to provide CUSTOMER NAME REMOVED with a SCCM environments with newly built Windows Server 2019 image.

Microsoft will provide Services in support of the following scope:

Table 90: General project scope

|  |  |  |
| --- | --- | --- |
| Area | Description | Assumptions |
| Workshops | * Microsoft will deliver up to 2 (two), 3-hour workshops to gather and document the design requirements for the SCCM environments. * The workshops will also be utilised to gather and document the design requirements for the Windows Server 2019 operating system. * Delivery 3 (one) 1-hour workshops for Windows Servicing | * CUSTOMER NAME REMOVED will make available the staff members required to participate in the educational workshops.   CUSTOMER NAME REMOVED will provide the facilities (room, whiteboard & projector) required for conducting the workshops. |
| Core SCCM Infrastructure | * The planning and design of the following Configuration Manager infrastructure that is used for on-premises:   + - 1 primary site     - Up to five (5) distribution points     - 1 reporting point * Role-based access administration * Implement one (1) client setting for hardware and software inventory, remote control, power management, and health attestation. | CUSTOMER NAME REMOVED will provide the infrastructure and servers for the implementation of SCCM |
| Windows Servicing | * Configure Windows server 2019 features and quality update management with Configuration Manager * Design and implement up to two (2) servicing plans for managing Windows 2019 semi-annual feature updates. | - |
| Windows Server 2019 Image | * Create the following Server 2019 Datacentre image using a single image design and the image factory:   + - 1 64-bit image (default)     - Inclusion of up to 5 applications in the image     - Configuration of up to 10 custom image settings * Installation of all publicly released and recommended updates through WSUS or Windows Update when the image is created * Implement additional plug-and-play device driver support for up to 5 makes and models of devices in Configuration Manager. | CUSTOMER NAME REMOVED will provide up to five (5) applications. Additional applications can be added via a Change Request. |
| Security Foundations | * Create a GPO that is based on a security baseline which include the following features:   + - Credential Guard     - Application Guard     - Exploit Guard     - Windows Defender Antivirus | - |

### Software products and technologies

The products and technology that are listed in the following table are required for project execution. CUSTOMER NAME REMOVED is responsible for obtaining all identified licenses and products.

Table 91: MSD - Software products and technologies

|  |  |
| --- | --- |
| Product and technology item | Ready by |
| Windows Server 2019 (latest version) | Two weeks prior to commencing the project |
| Windows Server 2012 R2 Standard (or later) for SCCM infrastructure (physical or virtual machines) | Two weeks prior to commencing the project |
| Microsoft SQL Server 2014 Standard or Enterprise Edition (Latest version) | Two weeks prior to commencing the project |
| System Centre Configuration Manager Current Branch | Two weeks prior to commencing the project |
| All CUSTOMER NAME REMOVED software to be deployed as part of the project (limited to up to 5 applications) | Two weeks prior to commencing the project |

### Environments

The following environments will be required to deliver this project

Table 92: MSD - Environments

|  |  |  |  |
| --- | --- | --- | --- |
| Environment | Location | Responsibility | Ready by |
| Production | CUSTOMER NAME REMOVED Datacentre | CUSTOMER NAME REMOVED | Start of the project |

### Testing

The following testing is included in the scope of the project. If CUSTOMER NAME REMOVED has responsibility for testing, the Microsoft effort to support that activity is identified. If additional time is needed for Microsoft testing support, then it can be requested through the change management process described in this SOW.

Table 93: MSD - Testing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test type (environment) | Description | Responsibility | | |
| Has responsibility  for testing? | Provides data or test cases | Provides guidance and support |
| System testing (SCCM Production environment) | Functionality testing focuses on determining whether functionality meets design. Test cases will be based on the technical guide document. (timeboxed to 1 day of effort) | Microsoft | Microsoft | CUSTOMER NAME REMOVED |
| Image UAT testing (in production) | Microsoft will test the deployment of the Windows 10 image onto devices provided by CUSTOMER NAME REMOVED (timeboxed to 2 days of effort) | Microsoft | Microsoft | CUSTOMER NAME REMOVED |

## Areas out of scope

Any area not explicitly included in the areas in scope section is out of scope for Microsoft during this project. Areas out of scope for this project, in addition to those listed elsewhere in this document, are listed in the following table.

Table 94: MSD - Out of scope

|  |  |  |
| --- | --- | --- |
| Area | Description | |
| All | * Design and implementation of a new Windows KMS infrastructure * Operating system upgrades of KMS servers, domain controllers, WSUS servers, or MDOP servers * Unsupported KMS servers * Creation of an Active Directory Domain Services (AD DS) group policy central store * Assessment, review, and modification of existing group policies * Design and implementation of a new servicing infrastructure using WSUS * Network and firewall configuration |
| Windows Servicing | * Third-party software update management * Feature update testing or quality update testing * Support for additional Microsoft products in Configuration Manager software update management * Windows Autopilot * Configuration and deployment of windows Analytics * Application portfolio discovery and rationalisation * Remediation of the existing environment and infrastructure. |
| Windows Image | * Evaluation of the image for regulatory compliance * Recommended practices that address compliance requirements * Identification of silent installation commands or creation of unattended installation scripts for application installers * Creation of scripts for automating image-setting customisation or configuration |
| Windows Deployment | * New device firmware preparation and configuration * Device driver remediation * Any existing hardware modification * Custom configuration XML files for the USMT * Any application compatibility testing or remediation * Identification of silent installation commands or the creation of unattended installation scripts for application installers * Creation of scripts for automating operating system settings, customisation, and configuration * Logistic and resource planning and allocation for deployment and migration activities |
| Security Foundations | * Design or implementation of security capabilities that are not listed in scope such as:   + - Windows Defender Advanced Threat Protection     - Windows Information Protection     - Device Guard     - Windows Hello for Business * Assessment, review, or modification of existing group policies * Creation of an AD DS group policy central store * Installation of new ADMX templates |

## Approach

The project will be structured following the Microsoft Online Services Lifecycle (OSL) methodology across three of the possible four distinct phases: Assess, Remediate and Enable. Each phase has distinct activities that are described in the following sections.

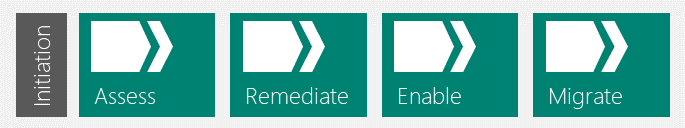


Figure 13: MSD - Approach

### Assess

During the Assess phase, Microsoft will conduct a series of workshops to gather design requirements. Microsoft, and CUSTOMER NAME REMOVED will review the results of the planning workshops and jointly determine requirements necessary to support the deployments.

Table 95: MSD - Assess phase

|  |  |  |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | **General activities**   * + - Conduct up to 2 (two), 3-hour decision-making workshops for each of the following services to gather requirements:     - Design & implement System Center Configuration Manager core infrastructure     - Design and pilot new or refresh deployment     - Design and implement Windows servicing     - Security foundations   **Infrastructure foundations**  Assess and validate the existing infrastructure:   * + - Activation (Windows KMS)     - ADMX templates     - WSUS     - MDOP solution   **Design and implement the servicing process**   * Workshop delivery: present up to three (3) workshops to CUSTOMER NAME REMOVED that can help define an approach to stay current with Windows as a Service. The workshops will include the following topics:   + - Compatibility     - Deployment (infrastructure, configuration, and operations)     - Capability and modernisation |
| **CUSTOMER NAME REMOVED** **activities** The activities to be performed by CUSTOMER NAME REMOVED | * Provide access to key personnel, service-level agreements, the current environment, and documentation. * Participate in workshops: provide detailed insights on application portfolio, infrastructure, configuration, and operational processes during design workshops to verify that appropriate guidance can be provided in the design document and implementation guide. * Plan and identify up to five (5) target devices or users for the deployment. * Prepare hardware client devices. * Prepare applications to be installed as part of the deployment. * Prepare test client devices. * Prepare device drivers. * Prepare the production environment infrastructure. |
| Key assumptions | * All required CUSTOMER NAME REMOVED personnel will attend workshops. * Decisions will be made during the workshops, by CUSTOMER NAME REMOVED to complete the final deployment and configuration process. * The network infrastructure is healthy. * CUSTOMER NAME REMOVED is aware of the existing corporate patching process and policies. * CUSTOMER NAME REMOVED is aware of the existing corporate standard image requirements and policies. * The latest System Center Configuration Manager Current Branch version will be installed. * CUSTOMER NAME REMOVED will perform necessary network and infrastructure changes to support the deployment. |

### Remediate

The remediate phase is not required for this project as the SCCM environment and Windows Server 2019 image will be built as new without legacy environments, migration or existing data.

### Enable

The Enable phase includes the production implementation of the solution and the initial 5 device deployment (to test the image). The 5-device pilot deployment will be deemed successful if each technical component passes the functional test criteria and test cases defined in the technical guide that was developed as part of the project.

Table 96: MSD - Enable phase

|  |  |  |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | **Design and implement Configuration Manager core infrastructure**   * Build the production Configuration Manager infrastructure and configure the environment; such activities include:   + - The configuration of 1 client setting     - Role-based access administration configuration   **Design and implement Windows servicing**   * Configure the following in the production environment and validate that they are working as designed:   + - Feature updates (either one): * Servicing plans for Windows 10 * GPOs   + - Quality updates (either one): * Automatic deployment rules * GPOs   **Windows Image**   * Create the following Windows Server 2019 reference image using a single image design:   + - One 64-bit image     - Configuration of up to 10 custom image settings * Install all publicly released and recommended updates through WSUS or Windows Update when creating the image. * Import drivers for up to 1 Virtualisation Platform.   **Windows Deployment**   * Implement the deployment task sequence in production and validate that it is working. * Import drivers for up to 1 Virtualisation Platform. * Perform an alpha deployment of 5 machines and support resolution of deployment problems within 5 working days. * Conduct a go-or-no-go meeting to review problems and resolutions related to deployment readiness.   **Security foundations**  Configure the GPO in the production environment and validate that the settings are applied to the devices. |
| **CUSTOMER NAME REMOVED** **activities** The activities to be performed by CUSTOMER NAME REMOVED | * Update the following production infrastructure and validate that the update has successfully completed:   + - Activation (Windows KMS)     - Administrative templates (ADMX) templates     - WSUS * Supply all hardware, virtual machines, operating systems built, and software required for the deployment of SCCM * Prepare the infrastructure for the Configuration Manager environment. * If necessary, verify the configuration of the network firewall, routers, and switches to permit standard client-to-server and server-to-server communication. * Infrastructure remediation—install, upgrade, or configure infrastructure configuration support services such as AD DS. * Remedy network services as required. * Remedy server problems as required. * Begin production backup and restore operations. * Assign a point of contact for each facility that has users who will be migrated. * Provide first-level and second-level support.   **Design and implement Windows servicing**   * Validate that the settings have been configured correctly and as designed.   **Windows Image**   * Provide all required software and licenses. * Provide the script or scripts needed to perform image-setting customisations. * Validate that the image created conforms to the design. * Validate that the image is functional. * Provide Windows 2019 supported drivers for the Virtualisation Platform.   **Security foundations**   * Validate that the policies have been applied correctly and do not conflict with existing policies. |
| Key assumptions | * The Active Directory replication and Domain name System infrastructure in production is in a healthy state. * Device will have internet connectivity * The Active Directory schema will be modified to include the System Center Configuration Manager site infrastructure according to System Center Configuration Manager installation recommendations. * Servers are joined to the Active Directory domain. * The latest Windows ADMX files are imported to the Active Directory central store. * Windows Update for business will be managed through GPO’s * CUSTOMER NAME REMOVED will provide source files and silent installation commands for all applications that will be included in images. * CUSTOMER NAME REMOVED will provide a silent script to configure the image settings * All target devices must be identified, remediated (if required), and prepared 1 week in advance of the scheduled deployment. * All existing devices have default admin shares activated. * All required CUSTOMER NAME REMOVED personnel will work with Microsoft during the system testing processes. |

## Deliverables

This section provides a list of the deliverables produced by the MSD project. If a deliverable requires formal review and acceptance (indicated by a Yes), it will be governed by the deliverable acceptance process as defined in section 2.5.

Table 97: MSD – Deliverables

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Phase** | **Deliverable name** | **Deliverable Description** | **Acceptance Required** | **Responsibility** |
| D43 | Assess | MSD Solution design document | Microsoft Word document that contains a description of the technical functionalities of the solution. | Yes  Acceptance Criteria:  A Microsoft Word document of approximately 100 to 130 pages, that accurately describes the solution design | Microsoft |
| D44 | Assess | MSD Preliminary test plan | Microsoft Word document that describes the strategy and approach that was used to plan, organise and manage the project’s testing activities. It identifies testing objectives, methodologies and tools, expected results, responsibilities and resource requirements.  The test plan details functional test cases for the solution and is provided in a preliminary format until the test cases have been completed and documented. | No | Microsoft |
| D45 | Assess | MSD Environment Information and Details | Details on the environment as well as infrastructure details for Microsoft to deploy SCCM | No | CUSTOMER NAME REMOVED |
| D46 | Enable | MSD Final Solution design document | Microsoft Word document that contains a description of the technical functionalities of the solution. | Yes  Acceptance Criteria:  A Microsoft Word document of approximately 100 to 130 pages, that accurately describes the solution design | Microsoft |
| D47 | Enable | MSD Final Test Plan | Microsoft Word document that describes the strategy and approach that was used to plan, organise and manage the project’s testing activities. It identifies testing objectives, methodologies and tools, expected results, responsibilities and resource requirements.  The test plan details functional test cases for the solution and is provided in a preliminary format until the test cases have been completed and documented. | Yes  Acceptance Criteria:  A Microsoft Word document of approximately 25 – 40 pages, that includes the expected test results and notes about implementing the defined test cases. | Microsoft |
| D48 | Enable | Up to five (5) servers | Up to five (5) production servers have been successfully deployed and tested | No | Microsoft |

## Project roles and responsibilities

The key project roles and the responsibilities are as follows.

### CUSTOMER NAME REMOVED

Required CUSTOMER NAME REMOVED Roles are defined at the Program level in section 3.2.1.

### Microsoft

Table 98: MSD - Microsoft Project roles and responsibilities

|  |  |
| --- | --- |
| Role | Responsibilities |
| MSD Consultant | * Participate in design and technical workshops. * Responsible for building the environment components and the required for the project. * Responsible for the 5-device pilot deployment. |

# P09: Operational Service Management (OSM)

## Objectives

The security controls introduced in this program of work, will change the way IT administers the various critical systems and the privileged accounts that control them.

This project is specifically designed to support CUSTOMER NAME REMOVED in understanding, adapting and operationalising the security practices that are being introduced, by:

* Discover and Analyse existing Admin Credential Support Practices and Tools
  + Assess current support processes and practices for risk exposure, and assist with integrating recommended practices into IT system administration and maintenance of PAW solution for Tier 1 and Azure Cloud
  + Assess current support processes and practices for risk exposure, and assist with integrating recommended practices into IT system administration and maintenance of the ESAE solution
* PAW Tier 1 and PAW Azure Cloud Support Roles and Process determination
  + Define Server support requirements and processes for Tier 1 and Azure Cloud
* Operations, Maintenance and Integration Planning.
* Plan PAW Tier 1 and PAW Azure Cloud support and operations integration into CUSTOMER NAME REMOVED’s existing Change, Configuration, Incident and Event Management processes. Create PAW Tier 1 and PAW Azure Cloud User and Admin Management Plan.
* Plan ESAE support and operations integration into CUSTOMER NAME REMOVED’s existing Change, Configuration, Incident and Event Management processes.
* Plan ATP (Azure, O365 and AD) support and operations integration into CUSTOMER NAME REMOVED’s existing Change, Configuration, Incident and Event Management processes.
* Assess, modify and implement the Windows 10 servicing update management
* Assess, modify and implement the Windows Server servicing update management

The overall objectives of this project are to confirm that CUSTOMER NAME REMOVED is operationally prepared to support and operate the ESAE environment, the PAW Tier 1 environment, the PAW Azure Cloud environment, the ATDIS service, the MDD environment and the MSD environment effectively, and to help CUSTOMER NAME REMOVED understand the IT Service Management processes and roles necessary for maintaining these environment in the same state and configuration as when it is deployed and turned over for steady-state support.

Table 99: OSM - Overall project objectives

|  |
| --- |
| Description of Objectives |
| * Prepare CUSTOMER NAME REMOVED ’s IT Operations and Service Management processes to operate and support the ESAE environment |
| * Prepare CUSTOMER NAME REMOVED ’s IT Operations and Service Management processes to operate and support the PAW environment (Tier 1 and Azure Cloud) |
| * Prepare CUSTOMER NAME REMOVED ’s IT Operations and Service Management processes to operate and support threat protection (ATP for Azure, O365 and AD) |
| * Develop needed operational processes and roles needed for secure administrative account management in the ESAE environment |
| * Develop needed operational processes and roles needed for operational management in the PAW environment (Tier 1 and Azure Cloud) |
| * Develop needed operational processes and roles needed for operational management for threat protection (ATP for Azure, O365 and AD) |
| * Facilitate CUSTOMER NAME REMOVED’s understanding of how to integrate the ESAE service into their existing support and operations processes |
| * Facilitate CUSTOMER NAME REMOVED’s understanding of recommended practices for maintaining the integrity of the ESAE solution |
| * Determine optimised support roles and processes for both Tier 1 and Azure Cloud PAW scenarios. |
| * Identify and document all technical and operational dependencies for the ESAE solution |
| * Identify and document all technical and operational dependencies for the PAW solution (Tier 1 and Azure Cloud) |
| * Identify and document all technical and operational dependencies for threat protection solutions (ATP for Azure, O365 and AD) |
| * Assess, modify and implement the Windows 10 servicing update management process |
| * Assess, modify and implement the Windows Server servicing update management process |
| * Facilitate CUSTOMER NAME REMOVED’s implementation and operationalising of identified Service Management processes and procedures with CUSTOMER NAME REMOVED’s administrators |

## Areas in Scope

### General Project Scope

Microsoft will provide services in support of the following scope:

Table 100: OSM – General project in scope

|  |  |  |  |
| --- | --- | --- | --- |
| Solution Component | Feature/Function | Description | Key Scope Assumptions |
| IT Service Management Support for ESAE | ESAE Operations and Maintenance | Discovery and analysis of current state operations processes | CUSTOMER NAME REMOVED will make available the necessary IT operations and process SMEs and documentation |
| Identify all technical and operational dependencies within and between the ESAE and standard production environments | CUSTOMER NAME REMOVED SMEs will participate in Service Mapping workshop and any needed follow-up interviews |
| Define roles and Responsibilities in support of ESAE and develop operational processes for secure Admin account management | SMEs will participate in workshops and interviews on current and future roles and responsibilities of support staff |
| User Account Provisioning | Development and creation of specific ESAE account provisioning process including policy or business rules | CUSTOMER NAME REMOVED will make available the necessary IT operations and process and documentation. The relevant stakeholders will participate in workshops and any needed follow-up interviews. |
| Development and creation of specific ESAE PAW provisioning process including policy and business rules | CUSTOMER NAME REMOVED will make available the necessary IT operations and process and documentation. The relevant stakeholders will participate in workshops and any needed follow-up interviews. |
| ESAE Integration | Assist in defining integration needs for existing support and maintenance processes: Incident, Request Fulfilment, Problem, Change, Release, Configuration and Event Management | CUSTOMER NAME REMOVED will make available the necessary IT operations and process SMEs, as well as decision makers for process and/or tooling modification |
| Transition support including assistance with transition documentation such as logistics and support planning and stakeholder engagement | CUSTOMER NAME REMOVED will make available the necessary transition process documents and a transition support SME that Microsoft will work to support.  CUSTOMER NAME REMOVED will provide a list of stakeholders and make stakeholders available to assist with transition and detail their transition requirements |
| Participate in test: validate, monitor and provide feedback into solution | Timely feedback on pilot experience to enable incorporation of lessons learned |
| Facilitate CUSTOMER NAME REMOVED’s implementation and operationalising of identified Service Management processes and procedures supporting ESAE and PAW Tier 1 with CUSTOMER NAME REMOVED’s administrators | CUSTOMER NAME REMOVED will make available the appointed administrators that will support BAU |
| IT Service Management Support for PAW (Tier 1 and Azure Cloud) | PAW Operations and Maintenance (Tier 1 and Azure Cloud) | Discover and Analyse existing Admin Credential Support Practices and Tools. Assess current support processes and practices for risk exposure and assist with integrating recommended practices into IT system administration and maintenance of PAW solution. | CUSTOMER NAME REMOVED will provide access to necessary documentation and/or IT operations SMEs, Process SMEs, and IT administrators. |
| Define Server support requirements and processes (Tier 1) and Azure support requirements and processes | CUSTOMER NAME REMOVED will provide access to necessary documentation and/or IT operations SMEs, Process SMEs, and IT administrators.  CUSTOMER NAME REMOVED will provide access to necessary decision makers for making changes to CUSTOMER NAME REMOVED environment. |
| Operations, Maintenance and integration Planning. Plan PAW support and operations integration into CUSTOMER NAME REMOVED ’s existing Change, Configuration, Incident and Event Management processes. | CUSTOMER NAME REMOVED will provide access to necessary documentation and/or IT operations SMEs, Process SMEs, and IT administrators.  CUSTOMER NAME REMOVED will provide access to necessary decision makers for making changes to CUSTOMER NAME REMOVED environment |
| Facilitate CUSTOMER NAME REMOVED’s implementation and operationalising of identified Service Management processes and procedures supporting ESAE and PAW Tier 1 with CUSTOMER NAME REMOVED’s administrators | CUSTOMER NAME REMOVED will make available the appointed administrators that will support BAU |
| IT Service Management Support for ATDIS | ATDIS Solution (ATP for O365, Azure, AD)) | Identify all technical and operational dependencies of the ATP environments | CUSTOMER NAME REMOVED SMEs will participate in Service Mapping workshop and any needed follow-up interviews |
| Review and update the Security Incident Management Process | CUSTOMER NAME REMOVED will provide access to necessary documentation and/or IT operations SMEs, Process SMEs, and IT administrators.  CUSTOMER NAME REMOVED will provide access to necessary decision makers for making changes to CUSTOMER NAME REMOVED environment. |
| Define roles and Responsibilities in support of ATP | SMEs will participate in workshops and interviews on current and future roles and responsibilities of support staff |
| Facilitate CUSTOMER NAME REMOVED’s implementation and operationalising of identified Service Management processes and procedures supporting ATDIS (including ATP for O365, Azure and AD) with CUSTOMER NAME REMOVED’s administrators | CUSTOMER NAME REMOVED will make available the appointed administrators that will support BAU |
| Service Management Support for Modern Desktop Deployment (MDD) | Modern Desktop Deployment (MDD) | Discovery and analysis of current state operations processes with a focus on software update management | CUSTOMER NAME REMOVED will make available the necessary IT operations and process SMEs and documentation |
| Identify all technical and operational dependencies of the MDD environment | CUSTOMER NAME REMOVED SMEs will participate in Service Mapping workshop and any needed follow-up interviews |
| Define roles and Responsibilities in support of MDD and develop operational processes for MDD | SMEs will participate in workshops and interviews on current and future roles and responsibilities of support staff |
| Facilitate CUSTOMER NAME REMOVED’s implementation and operationalising of identified Service Management processes and procedures MDD and MSD with CUSTOMER NAME REMOVED’s administrators | CUSTOMER NAME REMOVED will make available the appointed administrators that will support BAU |
| Service Management Support for Modern Server Deployment (MSD) | Modern Server Deployment (MSD) | Discovery and analysis of current state operations processes with a focus on software update management | CUSTOMER NAME REMOVED will make available the necessary IT operations and process SMEs and documentation |
| Identify all technical and operational dependencies of the MSD environment | CUSTOMER NAME REMOVED SMEs will participate in Service Mapping workshop and any needed follow-up interviews |
| Define roles and Responsibilities in support of MSD and develop operational processes for MSD | SMEs will participate in workshops and interviews on current and future roles and responsibilities of support staff |
| Facilitate CUSTOMER NAME REMOVED’s implementation and operationalising of identified Service Management processes and procedures MDD and MSD with CUSTOMER NAME REMOVED’s administrators | CUSTOMER NAME REMOVED will make available the appointed administrators that will support BAU |

## Areas Out of Scope

Any area that is not explicitly listed in Areas in scope section 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 101: OSM - Out of scope

|  |  |
| --- | --- |
| Area | Description |
| Process re-engineering | * Net-new Design of core operational or ITSM processes * Configuration of process or operational toolsets |

## Project Approach

### Envision

During the Envision Phase the team develops the ITSM portion of the project Vision & Scope that aligns expectations between the project team and stakeholders.

Table 102: OSM - Envision Phase

|  |  |
| --- | --- |
| Category | Description |
| Microsoft Activities | * Participate in Project Kick-off meeting * Participate in Envisioning workshop with project team * Discovery of current state operations processes * Identify high-level operations and process Integration Points that may need modification * Identify existing toolsets that enable IT support and operations processes * Conduct IT process and operations interviews * Identification of Operations and Delegation processes * Create ITSM portion of project Vision/Scope Document |
| CUSTOMER NAME REMOVED Responsibilities | * Attended kick-off meeting * Participate in Microsoft-led workshops, discovery activities, and any follow-on interviews |
| Exit Criteria | * Approval of Vision/Scope Document |
| Key Assumptions | * CUSTOMER NAME REMOVED will make available all needed Subject Matter Experts, decision makers and documentation |

### Plan

During the Plan Phase the team prepares needed changes and additions to CUSTOMER NAME REMOVED’s IT Operations Processes and Procedures, identifies changes to the roles and responsibilities associated with administrative accounts, security groups and PAW environment.

Table 103: OSM - Plan phase

|  |  |
| --- | --- |
| Category | Description |
| Microsoft Activities | * Create ESAE Service Map, RACI diagrams and Process diagrams * Create PAW Service Map, RACI diagrams and Process diagrams * Create ATP Service Maps (O365, Azure, AD) * Create MDD Service Map, RACI diagrams and SUM Process diagrams * Create MSD Service Map, RACI diagrams and SUM Process diagrams |
| Service Dependency Mapping (SMAP) | * Facilitate ESAE, PAW, ATP, MDD and MSD Service Dependency Mapping workshop * Conduct interviews and meetings to complete data gathering for SMAP * Create SMAP Excel spreadsheet and SMAP Visio diagram |
| Roles and Access Management | * Identify knowledge management (KM) requirements, processes and tooling for Roles and Access Management * Assist in determining and assigning Red Card admins * Assist in defining process for provisioning (request/approval/roles) new red card admins * Assist in determining and assigning Gold Card admins * Assist in defining process for provisioning (request/approval/roles) new gold card admins * Assist in determining process to clean out T0 admin groups * Assist in determining T1 admin support roles and groups for removed T0 admins * Assist in determining process for new membership in Tier 0 admin groups * Validate new support and operate processes for red and gold card admins (for Operations Guide) |
| Incident Management integration | * Identify knowledge management (KM) requirements, processes and tooling for Incident Management * Assist in determining appropriate priorities for ESAE, PAW T1, PAW Azure Cloud, ATDIS, MDD and MSD incidents * Define and document classifications, process flows and escalation matrices for ESAE, PAW T1, PAW Azure Cloud, ATDIS, MSD and MDD incidents, as well as any needed changes to existing toolsets |
| Problem Management integration | * Identify knowledge management (KM) requirements, processes and tooling for Problem Management * Identify known-error database needs for the Service Desk for ESAE, PAW T1, PAW Azure Cloud, ATDIS, MDD and MSD * Identify information needed in Incident Records to enable Problem Management for ESAE, PAW T1, PAW Azure Cloud, ATDIS, MDD and MSD * Update defined process flows for normal and major incidents into and through Problem Management * Define as needed: Request For Change (RFC) requirements, problem and error control, proactive problem management activities |
| Change Management Integration | * Identify knowledge management (KM) requirements, processes and tooling for Change Management * Map existing types of change to the anticipated changes introduced as part of the ESAE, PAW, ATDIS, MSD and MDD implementation. * Define and document process flows for types of changes for ESAE, PAW T1, PAW Azure Cloud, ATDIS, MDD and MSD components * Identify “Standard” changes anticipated for ESAE, PAW T1, PAW Azure Cloud, ATDIS, MDD and MSD - begin CAB pre-authorisation |
| Release Management Integration | * Identify knowledge management (KM) requirements, processes and tooling for Release Management * Define a Release Management Plan and schedules for ESAE, PAW T1, PAW Azure Cloud, ATDIS, MDD and MSD components * Define software update management requirements for ESAE, PAW T1, PAW Azure Cloud, ATDIS, MDD and MSD * Document process integrations with other support and operations processes (e.g., Change and Incident) |
| Configuration Management integration | * Identify knowledge management (KM) requirements, processes and tooling for Configuration Management * Guidance on controlling, status accounting and auditing for baselines * Document process integrations with other support and operations processes (e.g., Change and Incident, Event Management). |
| Event Management and Monitoring integration | * Identify knowledge management (KM) requirements, processes and tooling for Event Management * Identify key functional aspects of ESAE, PAW T1, PAW Azure Cloud, ATDIS, MDD and MSD components that need to be monitored * Provide guidance to monitoring team(s) on monitoring requirements for ESAE, PAW T1, PAW Azure Cloud, ATDIS, MDD and MSD * Define process workflows for ESAE, PAW T1, PAW Azure Cloud, ATDIS, MDD and MSD events from monitoring tools |
| CUSTOMER NAME REMOVED Responsibilities | * Participate in workshops and interviews and provide input to operational changes and additions as needed * Provide existing process and role documentation |
| Exit Criteria | * Delivery of ESAE, PAW T1, PAW Azure Cloud, ATDIS, MDD and MSD Service Maps. RACI diagrams and process workflows associated with Roles and Access Management |
| Key Assumptions | * CUSTOMER NAME REMOVED will provide access to SMEs, decision makers and operational Documentation as needed |

### Build

During the Build Phase the ITSM team builds a consolidated ITSM Process Integration Plan and integrates components of that plan into the ESAE Operations Guide and the PAW Operations Guide.

Table 104: OSM - Build phase

|  |  |
| --- | --- |
| Category | Description |
| Microsoft Activities | * Create ITSM Process Integration Plan * Integrate components of the Process Integration plan into the ESAE Operations Guide * Integrate components of the Process Integration plan into the T1 PAW Operations Guide * Integrate components of the Process Integration plan into the Azure Cloud PAW Operations Guide |
| CUSTOMER NAME REMOVED Responsibilities | Provide input into any draft plans and guides |
| Exit Criteria | Delivery of the ITSM Process Integration Plan and ITSM components of the ESAE Operations Guide and PAW T1 and PAW Azure Cloud Operations Guides |
| Key Assumptions | CUSTOMER NAME REMOVED staff will participate in sessions |

### Stabilise

During the Stabilise Phase testing is conducted and the team focuses on resolving issues and modifying final solution. The ITSM team will participate and provide feedback during the initial pilot. The ITSM team will also assist with establishing predictable, structured Service Review meetings.

Table 105: OSM - Stabilise phase

|  |  |
| --- | --- |
| Category | Description |
| Microsoft Activities | * Participate in pilot: validate, monitor and provide feedback into solution * Facilitate CUSTOMER NAME REMOVED’s implementation and operationalising of identified Service Management processes and procedures for ESAE, PAW T1, PAW Azure Cloud, ATDIS, MDD and MSD via MSM and technology consultants’ participation in go live activities, validating, monitoring and providing feedback (1-2 weeks per workstream) |
| CUSTOMER NAME REMOVED Responsibilities | * Gather pilot feedback and provide any lessons learned to the Microsoft team * Make relevant personnel and documentation available * CUSTOMER NAME REMOVED administrators that will support BAU will be available to ensure implementation and operationalising of identified Service Management processes and procedures. |
| Exit Criteria | * Known issues identified and feedback provided * Facilitation of CUSTOMER NAME REMOVED’s implementation and operationalising of identified Service Management processes and procedures |
| Key Assumptions | * CUSTOMER NAME REMOVED staff will participate in test phase and receive feedback * CUSTOMER NAME REMOVED will make available the appointed administrators that will support BAU |

## Deliverables

This section provides a list of the deliverables produced by the OSM project. If a deliverable requires formal review and acceptance (indicated by a Yes), it will be governed by the deliverable acceptance process as defined in section 2.5.

Table 106: OSM – Deliverables

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Phase** | **Deliverable name** | **Deliverable Description** | **Acceptance Required** | **Responsibility** |
| D49 | Envision | ESAE Vision/Scope Document (ITSM portion) | Explains the project ITSM vision and requirements | No | Microsoft |
| D50 | Plan | ESAE Service Map | Service Dependency Mapping Visio diagram and Excel spreadsheet | No | Microsoft |
| D51 | Plan | PAW Service Map | Service Dependency Mapping Visio diagram and Excel spreadsheet | No | Microsoft |
| D52 | Plan | ATP Service Maps (O365, Azure, AD) | Service Dependency Mapping Visio diagram and Excel spreadsheet | No | Microsoft |
| D53 | Plan | MDD Service Map | Service Dependency Mapping Visio diagram and Excel spreadsheet | No | Microsoft |
| D54 | Plan | MSD Service Map | Service Dependency Mapping Visio diagram and Excel spreadsheet | No | Microsoft |
| D55 | Plan | ESAE RACI diagrams | Roles and Responsibilities spreadsheets for roles delegation  Roles and Responsibilities spreadsheets from process integration work | No | Microsoft |
| D56 | Plan | PAW RACI diagrams | Roles and Responsibilities spreadsheets for roles delegation  Roles and Responsibilities spreadsheets from process integration work | No | Microsoft |
| D57 | Plan | ATP (O365, Azure and AD) RACI diagrams | Roles and Responsibilities spreadsheets for roles delegation  Roles and Responsibilities spreadsheets from process integration work | No | Microsoft |
| D58 | Plan | MDD RACI diagrams | Roles and Responsibilities spreadsheets for roles delegation  Roles and Responsibilities spreadsheets from process integration work | No | Microsoft |
| D59 | Plan | MSD RACI diagrams | Roles and Responsibilities spreadsheets for roles delegation  Roles and Responsibilities spreadsheets from process integration work | No | Microsoft |
| D60 | Plan | ITSM Process Flows | Process flow diagrams from Roles and Access Management work | No | Microsoft |
| D61 | Build | ITSM Process Integration Plan | Needed additions and modifications to existing IT operations and support processes, tooling, and roles and responsibilities | No | Microsoft |
| D62 | Build | ITSM components of the ESAE Operations Guide | Process Integration Plan inputs into the ESAE Operations Guide | No | Microsoft |
| D63 | Build | ITSM components of the PAW T1 Operations Guide | Process Integration Plan inputs into the PAW T1 Operations Guide | No | Microsoft |
| D64 | Build | ITSM components of the PAW Azure Cloud Operations Guide | Process Integration Plan inputs into the PAW Azure Cloud Operations Guide | No | Microsoft |
| D65 | Stabilise | Feedback and suggestions for modifications | Suggested modifications to processes, roles and tools | No | Microsoft |
| D66 | Stabilise | Facilitation of Implementation and Operationalising | Facilitation of CUSTOMER NAME REMOVED’s implementation and operationalising of identified Service Management processes and procedures via MSM and technology consultants’ participation in go live activities, validating, monitoring and providing feedback (1-2 weeks per workstream) | No | Microsoft |

## Project Roles and Responsibilities

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

### CUSTOMER NAME REMOVED

Required CUSTOMER NAME REMOVED Roles are defined at the Program level in section 3.2.1.

### Microsoft

Table 15: OSM - Microsoft Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| Role | Responsibilities | Project Commitment |
| Microsoft ITSM Architect | * Provide project oversight * Verifies whether Microsoft recommended practices are followed * Responsible for coordinating overall solution design | Part Time |
| Microsoft ITSM Delivery Consultant | * Operational design leadership * Delivery of all workshops and sessions for this project * Development of deliverables | Full Time |

# P10: Adoption and Change Management (ACM) Assistance

## Objectives

The objectives of this project are to achieve one or more of the following:

* An improved understanding of technology adoption challenges and the key next steps
* Resolution of a specific adoption issue that was defined at the onset and is addressed over the course of the engagement
* A defined roadmap to successful usage and adoption of new ways of working with Microsoft technology
* Identification and awareness of methods, tools, and the ability to measure the impact of behavioural change
* An enhanced capability to continue to drive behavioural change and measure its potential benefit on your own

## Areas in Scope

### General project scope

This is a fixed four (4) week engagement in which an ACM specialist will provide guidance on adoption and change management to CUSTOMER NAME REMOVED. See the Project approach and timeline section for more details.

### Areas out of scope

Any area not explicitly included in the areas in scope section is out of scope for Microsoft during this project. Areas out of scope for this project are listed in the following table.

Table 107: ACM - Out of scope

|  |  |  |
| --- | --- | --- |
| Area | Description | |
| Organizational change management | Designing—or redesigning—CUSTOMER NAME REMOVED functional organisation is not included. |
| User experience | Enhancements to the design of existing in-house applications and technical interface deployment are not in scope. |
| Branding | Corporate branding design and related graphic elements are not in scope. |
| Business case development | Business case creation for the technology investment is out of scope. |

## Project Approach

This project is comprised of three major milestones: a kick-off at the beginning, a progress review midway through the engagement, and a closeout meeting at the end of the project.

Deliverables that require formal review and acceptance (a process described in the Deliverable acceptance process section) are indicated in the following sections.

### Kick-off

During the project kick-off, the team (Microsoft and CUSTOMER NAME REMOVED) will define the focus of the activities of the ACM specialist and CUSTOMER NAME REMOVED. These activities would typically align to one to two of the following elements of the people side of change:

* Defined business outcomes, behavioural changes, and people impact
* Assessment of change management risk and cultural considerations
* Sponsorship, governance, and the change network
* Coaching and change management capability building
* Communications
* Training
* Measurement, reinforcement, and sustainability of change
* Behavioural insights strategy
* Resistance management
* Rewards and recognition
* Implementation planning
* Methods to connect change to outcomes

Table 108: ACM – Kick-off phase

|  |  |  |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | * Facilitate the kick-off meeting. * Present the recommended ACM approach. * Document engagement activities determined in collaboration with CUSTOMER NAME REMOVED. * Perform the activities agreed upon in the kick-off. |
| **CUSTOMER NAME REMOVED** **activities** The activities to be performed by CUSTOMER NAME REMOVED | * Attend and participate in the kick-off meeting. * Assign project initiation and responsibilities to accountable CUSTOMER NAME REMOVED leadership and establish target completion dates. * Complete project preconditions * Staff the project with the required CUSTOMER NAME REMOVED resources in the time frames that were agreed upon in the kick-off. |

### Progress review

Midway through the engagement, the ACM specialist will check in with CUSTOMER NAME REMOVED to track progress compared to the project activities and adjust, as necessary.

After the progress review, the ACM specialist will continue performing the engagement activities.

Table 109: ACM – Progress review phase

|  |  |  |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | * Perform the activities agreed upon in the kick-off. * Facilitate meeting. * Track the status of project activities and adjust accordingly. |
| **CUSTOMER NAME REMOVED** **activities** The activities to be performed by CUSTOMER NAME REMOVED | * Attend meeting. * Provide resources and information needed to complete the project activities. |

### Close out

At the end of the engagement, when the activities have been completed, the ACM specialist will provide CUSTOMER NAME REMOVED with the project results and recommended next steps.

Table 110: ACM – Close out phase

|  |  |  |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | * Perform the activities agreed upon in the kick-off meeting and discussed in the progress review meeting. * Facilitate meeting or exchange of information virtually (e.g. via email). * Document the project results and the recommended next steps. |
| **CUSTOMER NAME REMOVED** **activities** The activities to be performed by CUSTOMER NAME REMOVED | * Attend and participate in the closeout meeting. * Provide feedback on engagement activities. |

## Deliverables

This section provides a list of the deliverables produced by the ACM project. If a deliverable requires formal review and acceptance (indicated by a Yes), it will be governed by the deliverable acceptance process as defined in section 2.5.

Table 111: ACM – Deliverables

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Phase** | **Deliverable name** | **Deliverable Description** | **Acceptance Required** | **Responsibility** |
| D67 | Kick-off | ACM Project approach document | Documents agreement reached between the team and CUSTOMER NAME REMOVED on the desired activities and key success factors of the engagement. | Yes  Acceptance Criteria:  A Microsoft Word document that describes what was agreed to during the project kick-off. | Microsoft |
| D68 | Close out | ACM Closeout document | Documents completed activities and recommended next steps for the CUSTOMER NAME REMOVED ACM program. | Yes | Microsoft |

## Project Roles and Responsibilities

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

### CUSTOMER NAME REMOVED

Required CUSTOMER NAME REMOVED Roles are defined at the Program level in section 3.2.1.

### Microsoft

Table 15: ACM - Microsoft Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibilities |
| Microsoft ACM specialist | * Manage Microsoft ACM project delivery. * Take responsibility for Microsoft ACM resource allocation, risk management, project priorities, and communication with executive management. * Verify that deliverable development and activities are completed according to the plan. * Provide thought leadership in ACM. * Delivery of ACM sessions, workshops, classes, work products, and deliverables. |

## Project assumptions and preconditions

A critical success factor for this ACM project is visible, active commitment and involvement from all business sponsors and stakeholders. Work behaviour changes cannot be successfully implemented through external guidance alone; an organization can only change itself from within, and it requires dedicated resourcing and relentless focus through determined participation and perseverance.

In order for the underlying business goals to be met, an effective partnership between the Microsoft delivery team and your team is required. That partnership relies on certain preconditions being met, so that when the ACM program starts, it can be implemented without delays caused by a lack of readiness from either a technology or organizational perspective.

The following list of preconditions is minimum guidance.

Fulfilment of the preconditions will be checked as part of this engagement’s Assessment phase. Any omissions will likely cause delays in the program or in its expected effect until they are remediated.

### Preconditions

At a minimum, the following list of preconditions must be met by CUSTOMER NAME REMOVED to help make sure CUSTOMER NAME REMOVED receive the full benefit of the program:

* Business stakeholders and decision makers who have the capabilities and qualifications necessary to guide and take responsibility for the activities stipulated in CUSTOMER NAME REMOVED roles above.
* An IT sponsor has been named and is committed to the sponsorship role.

# Conclusion

The Cybersecurity Response Program (CRP) outlined in this Statement of Work is intended to assist CUSTOMER NAME REMOVED with addressing the identified critical and high-rated risks associated with the management of privileged access accounts across the bank.

Microsoft’ Active Directory technology is the glue that connects Users, Devices and Applications together, making it a highly attractive target for adversaries’ intent on operating advanced persistent threats within the bank’s environments.

Therefore, the combination of Microsoft recommended practice architecture and design, combined with leveraging the latest identity and security foundational technologies from Microsoft, will result in a new operating model that will significantly reduce the bank’s current risk position as it relates to the management of privileged access accounts.

Finally, Microsoft will also provide a roadmap and plan for the bank to evolve its current security posture from a “castle and moat” network perimeter based model towards a “zero trust” network model, which is the key security paradigm transition needed by the enterprise to participate in the evolving API economy and leverage cloud services (i.e. the perimeter-less enterprise).