POL00337657

EUC MANAGED SERVICES

Service Specification Document

POL00337657

CONTENTS

1. ABOUT THIS DOCUMENT 5
   1.1 Introduction and document structure 5
   1.2 Glossary 7
2. INTRODUCTION 11
   2.1 The Post Office Limited 11
3. OVERVIEW OF THE POST OFFICE REQUIREMENT 12
   3.1 EUC Drivers for Change 13
   3.2 Post Office Branches Userbase Overview 14
   3.3 Colleague Userbase Overview 18
4. TECHNOLOGY FRAMEWORK 20
   4.1 Technology Framework Overview 20
   4.2 Shared Services 20
   4.3 Branch Technologies 27
   4.4 Test and Release 31
   4.5 Colleague Technologies 37
5. SERVICE OPERATING MODEL 46
   5.1 Post Office Service Support Operating Model 46
   5.2 Incident Management 49
   5.3 Major Incident Management 50
   5.4 Incident Priority Definitions 50
6. SERVICE SPECIFICATION 59
   6.1 Service Operating hours 59
   6.2 Architecture 60
   6.3 Cloud / Infrastructure Management & Support 63
   6.4 Engineering Services 69
   6.5 Build, Software Packaging & Release Management 76
   6.6 Service Management 83
   6.7 Service Operations 91
   6.8 End User IMACD 99
   6.9 Security 104
   6.10 Project Services 108
   6.11 Monitoring and Reporting 114
7. SERVICE LEVELS AND KEY PERFORMANCE INDICATORS 120
   7.1 Service Level Agreements 121
   7.2 Key Performance Indicators 129
8. TOOLING 143

POL00337657

8.1 List of Tools 143
9. IMPLEMENTATION 147
9.1 Implementation Overview 147
9.2 Implementation Objectives 147
9.3 Implementation Principles 147
9.4 Implementation Services 147
9.5 Implementation Delivery Approach 148
9.6 Implementation & Integration 148
9.7 Service Operation 148
9.8 Change 149
9.9 Process & Procedures 149
9.10 Security 149
9.11 Business Continuity & Disaster Recovery 149
9.12 Transition of Staff (Relevant Transfers) 149
9.13 Business Communications 150
9.14 Implementation Governance 150
9.15 Reporting 150
9.16 Supplier Implementation Team 150
9.17 Document Deliverables 151
9.18 Implementation Milestones 163
9.19 Implementation Schedule 163
9.20 Acceptance Criteria 164
9.21 Testing 164
9.22 Change Freeze 165
10. TRANSFORMATION 166
10.1 Transformation Overview 166
10.2 Phases of Transformation Project 166
10.3 Project Governance 166
10.4 Change Freeze 166
10.5 Colleague Windows 10 Upgrade Project 166
10.6 Shared Services Separation Project 173
10.7 Analytics Project (Exercisable Option) 178
10.8 Remote Device Management (Exercisable Option) 181
11. POST OFFICE FUTURE ROADMAP / PROJECTS 186
11.1 Post Office Future Roadmap / Projects Overview 186
11.2 Strategic Platform Modernisation 186
11.3 Microsoft 365 E5 186
11.4 CviT (Cash & Valuables in transit) Drivers PDA Replacement 187

POL00337657

12. GOVERNANCE 188
12.1 Summary of Service Specification Governance / Meeting Requirements 189
13. APPENDIX A – LIST OF DOCUMENTS 191

POL00337657

1. ABOUT THIS DOCUMENT

1.1 Introduction and document structure

This document has been produced as part of the Further Competition pack, for the Post Office Ltd End User Computing (EUC) Services tender, under the Crown Commercial Services RM3804 Technology Services 2 Framework. The SSD is written to convey the service specifications for the Post Office EUC Colleague and Branch IT services to potential Suppliers in order to allow them to effectively bid on the respective supply of services to the Post Office.

This document forms part of the complete Further Competition documentation set, as illustrated on the following page in Figure 1. Post Office EUC Tender Documentation Structure.

Document Section	Purpose
Section 1 About this document	Description of the purpose of the SSD and its relationship to the other Further Competition tender documents.
Section 2 Introduction	Provides an initial introduction to the Post Office Limited and our key aims.
Section 3 Overview of the Post Office Requirement	Introduction to the Post Office EUC Services requirement, the key change drivers and the overview of the Branch and Colleague areas of the Post Office business.
Section 4 Technology Framework	Provides a detailed description of the technology used across the Post Office and which is in-scope for the EUC Supplier.
Section 5 Service Operating Model	Details of the Post Office Service Operating Model including the internal Post Office IT team areas, the high-level roles and responsibilities.
Section 6 Service Specification	Detailed definition of the EUC Services requirements, these services apply to the scope of the Technology Framework.
Section 7 Service Levels Agreements and KPIs	Describing the required Service Level Agreements and Key Performance Indicators in relation to the Services.
Section 8 Tooling	Description of the key toolsets which the supplier is required to use/integrate with, or provide input data feeds for.
Section 9 Implementation	Provides the requirements for the Implementation of the Supplier EUC Services solution to deliver the Run state requirements under the new contract.
Section 10 Transformation	Details of requirements for the in-scope Transformation projects which the supplier will be required to implement.
Section 11 Post Office Future Roadmap / Projects	An overview of additional changes and projects which the Post Office are likely to implement in the future, and which may require the assistance of the EUC Supplier, but do not form part of the initial scope.
Section 12 Governance	Summary diagram of the key Governance forums which are specified in the individual Service Specification section.
Appendices	Supporting data and reference documents for the SSD.

Table 1: *Service Specification Document Sections*

IMPORTANT NOTE TO SUPPLIERS:
Suppliers should ensure they have read all sections of this document and all related documents including the referenced Post Office documents in Appendix A, the Further Competition ITT, the draft Order Form, as well as the CCS framework T&Cs, Call Off contract T&Cs and the selected Additional T&Cs, before raising questions.

POL00337657

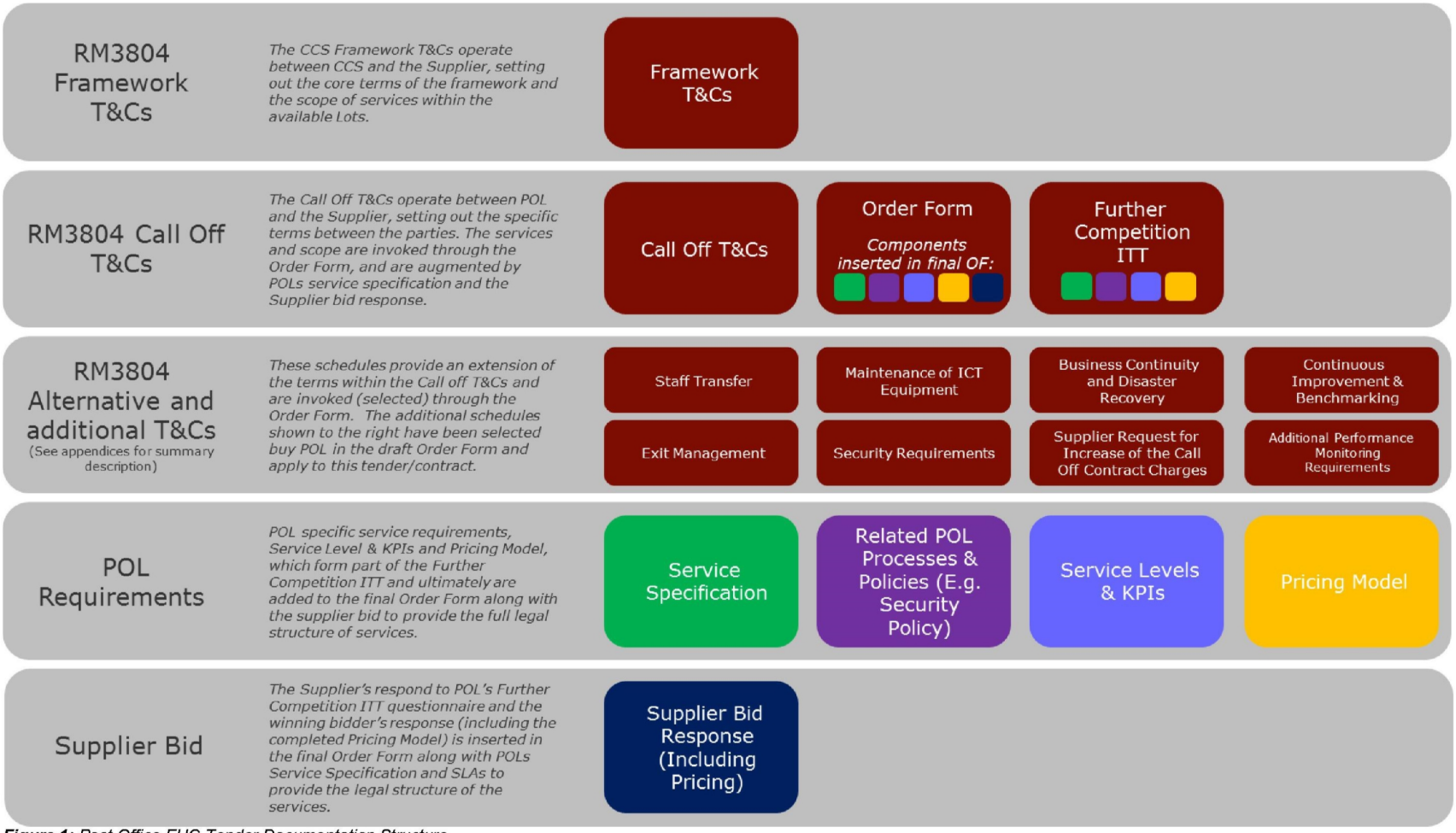


Figure 1: *Post Office EUC Tender Documentation Structure*

POL00337657

1.2 Glossary

In this Service Specification the following words and phrases have the following meanings:

Term	Definition
AAD Hybrid	Azure Active Directory Hybrid
ADFS	Active Directory Federated Services
Admin	Referring to the Post Office Colleague estate, some documentation may contain a legacy name of 'Admin' which equates to the Colleague part of the Post Office Business
ADSL Routers	Asymmetric Digital Subscriber Line Routers
Android tablet MDM	Android Tablet Modern Device Management
AEI	Application Enrolment & Identity
AGMP	Advanced Group Policy Management Tool
API	Application Programming Interface
AV Device	Audio Visual Device
AWS	Amazon Web Service
AWS SEC	Amazon Web Service Security
AWS Sec Hub	Amazon Web Services Security Hub
BAU	Business as Usual
BC/DR/HA	Business Continuity/Disaster Recovery/High Availability
BYOD	Bring your own device
CAB	Change Authority Board
CCS	Crown Commercial Service
CDU	Counter Deployment Utility
CFS	Core Finance System
Change Freeze	Periods of time around where changes cannot be made to the IT estate, usually Christmas and End of Year but exact dates to be confirmed by the Post Office
CI	Configuration Item
CISCO	Trade name, manufacturer of networking & security products
COA	Customer Operational Architect
CMDB	Configuration Management Database
Counter Deployment OSD	Operating System Deployment
Counter PoS	Counter Point of Sale
CViT	Cash and Value in Transit
DB Services	Database Services
DBS Check	Disclosure and Baring Check
DHCP	Dynamic Host Configuration Protocol
DMB	Directly Managed Branch
DMBs	Directly Managed Branches
DNS	Domain Name System
DOCX	Microsoft Word file suffix, as in "filename.docx
EOL Status	End of life status
e2e	End to End
DR&ITSM Commitments	Disaster Recover and Information Technology Service Management Commitments

POL00337657

End User IMACD	End user Installation Move Addition Change Deletion
Enhanced Support	A level of end user support that goes above the standard support model and provides a VIP one-on-one integration usually in person
EUC	End User Computing
Feature updates	Technically new versions of Windows 10, which become available twice a year (roughly every six months) during spring and fall.
FMI	SAP Financial Management Information
GDPR	General Data Protection Regulation
GLO IT	Group Litigation Order Information Technology
GPO	Group Policy Object
GUI	Graphical User Interface
HNGA	Horizon Next Generation Anywhere (Terminal device on the counters)
HR SAP	Human Resources Statutory Accounting Principles
IaaS	Infrastructure as a Service
ICT	Information and Communications Technology
IMACD	Installation Move Addition Change Deletion
Incidents MIM	Incidents Major Incident Management
IPAM	IP Management tool
IP Management	Internet Protocol Management
IPSEC	Internet Protocol Security
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
ITSM Toolkit	Information Technology Service Management Toolkit
ITT	Invitation to Tender
KPI	Key Performance Indicator
KVM	Keyboard Video Mouse
Labels	Used for labelling mails items and home shopping returns
LPOSS	Legacy Point of Sale System
LST	Live System Test
LTSB	Windows 10 "Long Term Servicing Branch"
LTSC (Windows 10)	Long-Term Servicing Channel
MBAM	Microsoft Bitlocker Administration & Monitoring
MDOP MBAM	Microsoft Desktop Optimisation Pack that includes a few tools including Microsoft BitLocker Administration and Monitoring (MBAM) which provides an administrative interface to enterprise-wide BitLocker drive encryption.
MDT	The Microsoft Deployment Toolkit
MDT Build	Microsoft Deployment Toolkit Build
MDM	Master Data Management
MFA	Multi Factor Authentication
Microsoft Defender ATP	Microsoft Defender Advance Threat Protection
MITRE ATT& CK Framework	A framework which helps organisations manage cyber risk better and plan what data needs to be available for cyber threat detection or investigating a security incident
MSI &APP-V	Microsoft Installer & Microsoft Application Virtualization

POL00337657

NDES Cert	Network Device Enrolment Service
NetBIOS	Network Basic Input Output System
PAM	Privileged Access Management
PAT Testing	Portable Appliance Testing
Patch and S/W Release	Patch & Software Release
PC	Personal Computer
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standards
PCI Legislation	Payment Card Industry Legislation
PCI SSC	Payment Card Industry Security Standards Council
PID	Project Initiation Document
PIM/PAM	Privileged Identity Management / Privileged Access Management
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKI Cert	Public Key Infrastructure Certificate
PKI Cert Services	Public Key Infrastructure Certificate Services
POG	Post Office Group
POL	Post Office Limited
Post Office SAP	Post Office Limited Statutory Accounting Principles
Post Office SOC	Post Office Limited Security Operations Centre
PPE	Pre-Production Environment
PSU for Branch Devices	Power Supply Unit
RACI	Responsible, Accountable, Consulted, Informed
RAID	Risks, Assumptions, Issues, Dependencies
RBAC	Role Based Access Restrictions
Receipts	Records of a service purchase or a banking withdrawal/deposit
Retail	Referring to the Post Office Branch areas of the business. Branch and Retail are used interchangeably in the Post Office Business.
RDT	Reference Data Test Environment
RFC	Request for Change
RTO/RPO/RTA	Recovery Time Objective/ Recovery Point Objective / Recover Time Actual
SACM	Service Asset & Configuration Management
SCCM	System Centre Configuration Manager used for Client Management
SCEP	Single Certificate Enrolment Protocol
SecOps	Security Operations
SEPAV	Symantec Endpoint Protection Antivirus.
SIAM	Service Integration & Management
SIEM	Security Information and Event Management
SME	Subject Matter Expert
SOAR Functions	Security, Orchestration, Automation and Response Functions
SOC	Security Operations Centre

POL00337657

Software Distribution (MSI & APP-V	Microsoft application package installation formats
SQL Server	Sequel Server
SSO	Single Sign On
SubCA	Sub Certificate Authority
SV&I Environment	Solution Validation and Integration Environment
T&C's	Terms and Conditions
Transtrack CWC	Transtrack Cash Web Community
TLS	Transport Layer Security
Traka 32	Support software for Traka cabinets which provides graphical representation of the cabinets and allows users easy visual on activities happening on each Traka cabinet
UAT	User Acceptance Testing
VSAT	Very Small Aperture Terminal. (It is the satellite dish connection to the internet.)
VIP Engineer	Very Important Person (Engineer)
VNet Peer	Virtual Network Peering
VPN	Virtual Private Network
VPN Clients	Virtual Private Network Clients
Windows 10 LTSC	Windows 10 Long Term Servicing Channel
2FA	Two Factor Authentication

Table 2: *Glossary of key terms*

POL00337657

2. INTRODUCTION

2.1 The Post Office Limited

We're here, in person, for the people who rely on us

"We're here"

- UK-wide physical presence is our strongest differentiator.
- Our strategy must right size the network: providing the right services in the right place at the right time.
- We are the UK's largest retail network with circa 11,400 branches.
- 90% of people in the UK live within one mile of a Post Office branch.

"In person"

- Postmasters are the Post Office. There is no Post Office without them. They should be at the heart of everything we do.
- Postmasters serve our Customers reflecting the diverse communities they serve.
- Everyday Postmasters and Customer-facing colleagues are making important, personal and human connections with the Customers and communities they serve. That human, personal touch is what makes us different.
- Post Office Limited's role is to be here for Postmasters – supporting and working with them to deliver for Customers and corporate clients.
- This doesn't mean that we are turning our back on digital or online. Digital and automation will always be an important enabler of our physical services, however, at our core, we are here, to serve people, in person.

"For the people who rely on us"

- This refers to our core Customers – those who rely on us.
- In the past, we have tried to appeal to everyone – we have lacked focus and prioritisation.
- We must accept that not everyone needs us every day. However, everyone needs the Post Office at some point in their lives.
- As the world changes around us, some people will rely on us more than others. For example, as retail bank branches close on the high street, we will need to be there to carry out banking services.
- We are relied and depended upon to deliver simple, trusted services for people, small businesses and our corporate Customers when they need them.

POL00337657

3. OVERVIEW OF THE POST OFFICE REQUIREMENT

The current Post Office End User Computing (EUC) services are supported under the current contract until 29th April 2021.
The contract includes a 'Termination Services' provision allowing the services within this contract to continue beyond the 29th April 2021 so they may be maintained whilst the Post Office moves to the EUC services model defined in our EUC Services specification.

There are three distinct phases of the EUC contract - Implementation, Run and Transformation. This Service Specification Document describes the requirements of each of these phases and the related Technology Framework, as summarised in the below diagram:

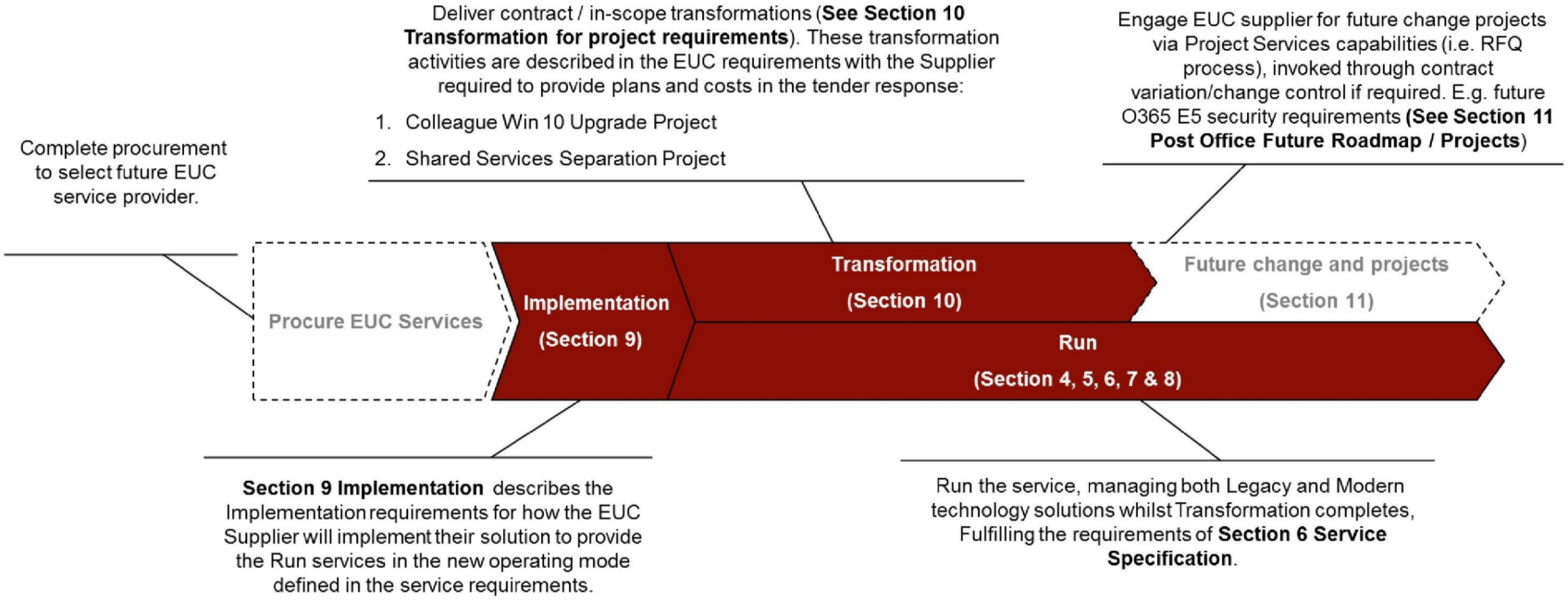


Figure 2: *EUC contract phases and relationship to SSD sections)*

The following section provides a summary of our End User Computing key drivers for change and a high-level overview of the Colleague and Branch areas of the Post Office business.

POL00337657

3.1 EUC Drivers for Change

The Post Office is split into Colleague and Branch, with Colleague representing the Post Office corporate and administrative organisation and Branch representing the Post Office retail organisation that serves the public.

Whilst the Post Office is seeking a single EUC supplier to deliver the requirements of this tender, these areas are operated as distinct business areas within Post Office Limited and will need to be clearly distinguished with regards to services, service levels and costs delivered through the EUC contract.

The renewal of our EUC contract provides an opportunity to re-think and re-implement the structure and ways of working for EUC services, which will help to deliver our current and future business needs, providing a more agile, more targeted and more commercially competitive service for the Post Office, our postmasters and our staff.

We want to put the Postmaster first:

- The traditional retail Branch environment is under significant external pressures with increasing competition. There is a continued expectation that systems are stable, always available when our Postmasters need them, highly robust and transparent.
- Our services need to be delivered to Postmasters with a proactive care, avoiding or mitigating issues and events which impact a Postmaster.
- We need to ensure services are underpinned by strong service level agreements which represent not only reactive targets but should also reflect Postmaster service satisfaction.
- Our Postmasters need an effective support solution, both via remote support and also through field engineering services, whereby, engineers visit Branches in order to perform routine services such as IT tasks required to set up branches, maintain systems and equipment or perform break-fixes/replacements quickly so Postmasters can continue to provide their services to Customers.
- We need IT change managed in a way which is reflective of the size and diversity of the Post Office Branch network.
- We expect our field engineers to be the face of Post Office IT and provide help with routine maintenance and be a representative of the wider Post Office brand to the Postmasters.

We want to ensure we have Colleague Focused Services:

- Within Post Office Colleague we want to be able to adapt to business needs quickly, recognising the different service needs in Colleague compared to Branch.
- Our Colleague systems need to be secure, available and kept updated for our staff.
- We want to drive transformation in Colleague in order to gain the benefits of modern device management and further adoption of cloud services, providing more dynamic access to Post Office systems.
- We want to maximise flexibility in terms of home and office working, recognising the long-term need for different working styles.
- We want future flexibility to extend services to the wider Post Office Group (POG) if corporate synergies can be found.

POL00337657

We want to Implement a Technical Separation of EUC Shared Services:

The 'back office' systems required to run Post Office laptops and desktops are currently combined for Colleague and Branch as 'Shared Services'. By separating these out into Branch and Colleague component parts, we will:

- Allow Colleague change to be more agile and quicker paced.
- Create a clear and real airgap between Colleague and Branch systems, removing the risk of change relating to one area impacting the service performance, availability and resilience of the other.
- Allow the Branch technology strategy and the Colleague technology strategy to select the technical platform / tools which will best meet the needs of their respective business areas (allowing technical divergence between Branch and Colleague where this is beneficial).

We would therefore like to technically separate the two estates to better facilitate the corresponding strategies for each part of the business. This driver reflects the very different parts of the Post Office business and the different levels of technical complexity and diversity.

We want specialist partners to achieve our aims:

To achieve our aims, we need the right partnerships and specialist suppliers in place. We want an EUC supplier who will:

- Be fully accountable for their services, driving innovation and improvement.
- Deliver the core services consistently and competently with skilled resources and specialisms.
- Provide strong management controls and proactive behaviours. Our suppliers must excel in planning, checking, rehearsing and validating delivery of the services and in change activities needed for our Post Office business.
- Be straightforward and direct with communications.
- Cooperate seamlessly with our organisation and wider supplier network.
- Routinely and consistently demonstrate and report delivery of Post Office's EUC Service requirements and quality expectations.

We are therefore asking Suppliers of the Crown Commercial Services RM3804 Technology Services 2 framework to submit proposals for how they would manage the required services which are detailed within this document.

3.2 Post Office Branches Userbase Overview

The EUC contract supports the hardware, core software builds, build updates with feature releases, security patching, software and hardware asset management including chain of custody for PCI-DSS items, and field engineering services across the Post Office Branch network.

The Post Office Branch Network represents a substantial footprint of approximately 11,400 active branches nationally across the UK with circa 25,000 counter positions. These 11,400 branch locations are the active service points or 'Branches' which include remote /outreach

POL00337657

locations such as village halls and Post Office 'In a Van' services. Each outreach location is homed on a Post Office Shop location, or 'Home' location, and hence multiple outreach locations will be related to a single Home location. As such there are currently circa 10,000 Post Office Branch / Home locations which are in scope of this EUC Contract, but this exact number varies through the process of branch opening, change and closures (see Section 6, Service Specification: Operational Business Change (OBC).

Full details of the Post Office Branch / home locations are provided in **Appendix A: Ref Doc- 007 Branch and Colleague Locations.**

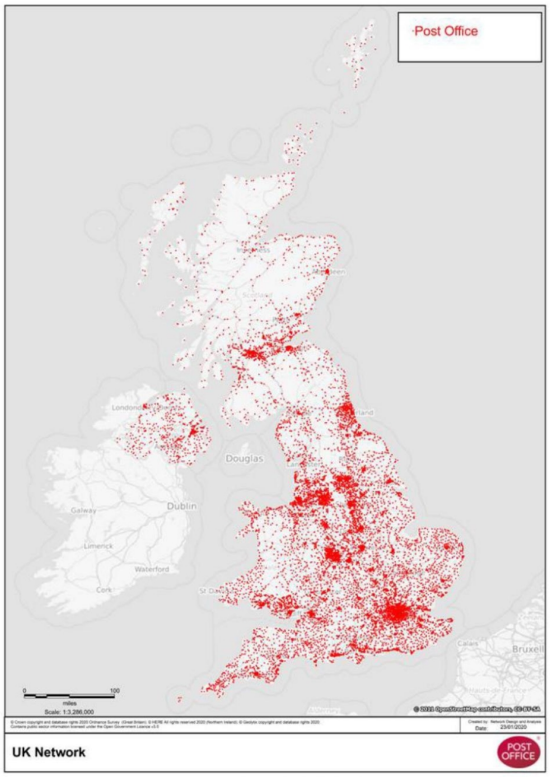


Figure 3: *Branch UK Network*

The impacts of the global Covid-19 pandemic resulted in some branches temporarily closing, and Post Office will be actively growing the network to return to the required BEIS target of 11,500 active branches.

As part of modernisation and improvement activities, branches are categorised into a small number of "Branch Types". This enables the Post Office to target IT solutions to the individual needs and challenges of this wide and diverse retail environment.

Whilst the exact number and the ratio of types of branch will change over time, to provide Suppliers with an indication of the ratios of branch types, the current branch types are:

DMB – Total: c118 A "Directly Managed Branch" is a traditional branch model where the staff are managed directly by Post Office Limited. These branches have connectivity to the Colleague environment to enable the Branch to access Post Office colleague technologies e.g. corporate email services and Windows 8.1 laptops.

POL00337657

Main – Total: c3,400 A 'Main Branch' is a large multi-counter Branch which is run by a franchisee agreement. A 'Mains Post Office' is designated as such because it is designed to offer a modern environment and, in many cases, extended opening hours. These branches have dedicated Post Office counter(s) offering Customers a full range of products and services, during standard hours. In most cases there will also be Post Office service provisions at the retail position, providing access to a wide range of services including Post Office Card Account withdrawals and everyday banking services during extended opening hours. These branches are expected to have larger footfall and transaction volumes.

Local & Local + – Total: c4,200 A ' Local Model Branch' is usually situated in a Retail Environment and a lower number of counter positions (between 1 and 3). Also known as a 'Local Post Office'. It will carry a set product range which is a subset of the full range that a Main post office would offer. These branches are open when the shop it is housed within is open.

Traditional – Total c2100 All other Post Offices that are not one of the defined branch types

Outreach / Access Points– Total: 1,600 Post Office provide 'outreach' post office services to remote rural communities. This includes those operated out of local buildings, such as village halls or community centres, and the fleet of 59 mobile post office vans serving over 520 communities. Mobile Post Offices visit communities at a set time on set days and provide a walk-in service on wheels.

Others – In addition there are other formats of branches which are included in the above figures such as British Forces Post Offices (BFPO's) and non-customer facing branches e.g. House of Commons.

A full list of Post Office Branch locations is provided in **Appendix A: Ref Doc- 007 Branch and Colleague Locations.**

POL00337657

3.2.1 Branch Counter Device Overview

The following is a high-level summary description of the Branch Counter equipment. A detailed technical breakdown is provided in **Section 4: Technology Framework.**

Note - the point of demarcation between the EUC and Network Supplier is the egress of the Branch router.

Device Name	Description	Branch Type
Branch Counter	Point of Sale device used at counters to process Customer transactions. These include: • Base unit (BoxTech Cielo tablet or Lenovo M79 / PX-35) • The till operating system is "kiosk" version of Windows which is Windows 10 LTSC • Bar Code Scanner • Multifunction printer (Receipts and Labels) - Epson TM7200 – Designed for Post Office • Specialised Keyboard = Tipro Keyboard - TIP-002-999 • Electronic Scales (may be shared between counters at 2:1 ratio) • Pin Entry Device (Ingenico IPP350) • Scales Connector (shared between counters)	All
AEI	• KVM Switch for Application Enrolment and Identity (AEI) booths. The KVM Switch is used to switch between a normal Horizon transaction and a AEI transaction	Some branches (1000)
Identity Tablets	• Identity Tablets managed by MS Endpoint Manager (Intune) This includes Device Management, App Management, Security Management, Content Management, Email Management and Containerisation	Currently 800 Devices
Backoffice Counters	A Backoffice counter that is used for drop and go, balancing and stock ordering	Some Branches
Backoffice Printer	Canon A4 printer used for account balancing and report purposes	All Branches
8 Port Hubs	Hubs providing internal network connectivity for branch connected devices.	Some branches

Table 3: *Summary description of the Branch Counter equipment*

POL00337657

3.3 Colleague Userbase Overview

There are approximately 3325 directly employed staff in Post Office. 38% of this headcount is based across five primary sites (Finsbury Dials in central London, Future Walk in Chesterfield, Birmingham CVIT, Wheatstone House Swindon, and PS Service Centre Bolton. The remainder (47%) are based across multiple sites such as cash processing centres and stock management warehouses. A small number of staff will also be based in premises which are also shared by Directly Managed Branches (DMBs).

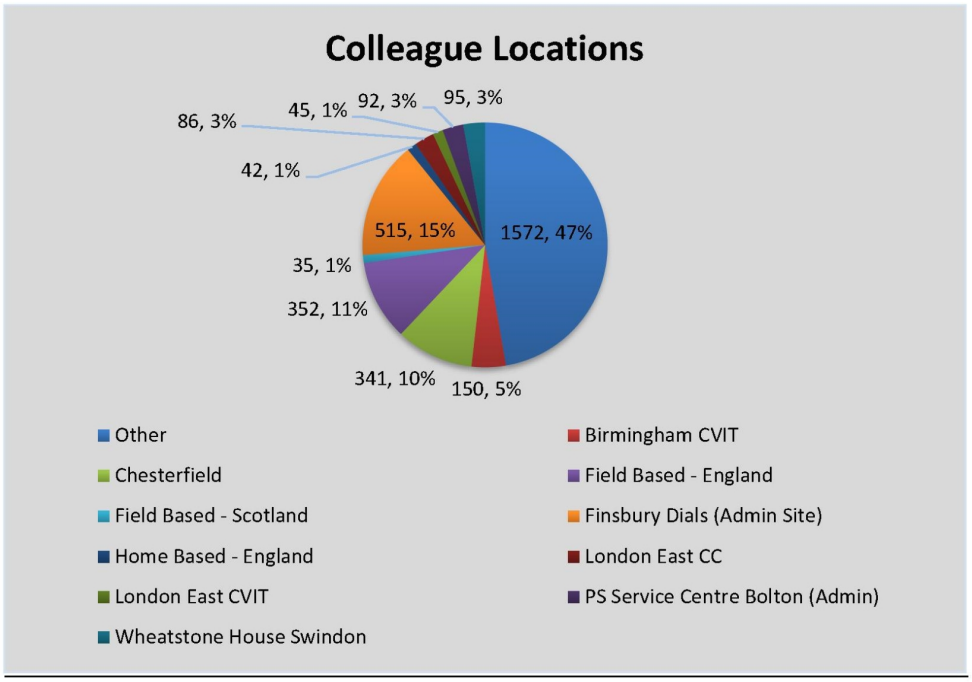


Figure 4: *Colleague locations*

The total number of Colleague locations is 154 and of these about 131 have 20 Colleagues or less.

The mix of location and staff numbers during business as usual operation was 43 (1%) of colleagues were home-based, 352 (11%) of Colleagues were field based (England) and 1% (Scotland). Due to the impact of Covid-19 restrictions and the Post Office's need for compliance and continued delivery of key services to our Customers, around 99% of head office staff have pivoted to home working.

In the vast majority of cases, resolution of Colleague related issues prior to, and throughout Covid-19 operations is achieved remotely, accepting that some equipment delivery/ collection is completed by the EUC Supplier.

A full list of Colleague Office locations is provided in **Appendix A: Ref Doc- 008 Branch and Colleague Locations**

Consumers of Colleague IT Services can be broadly separated into seven Personas;

POL00337657

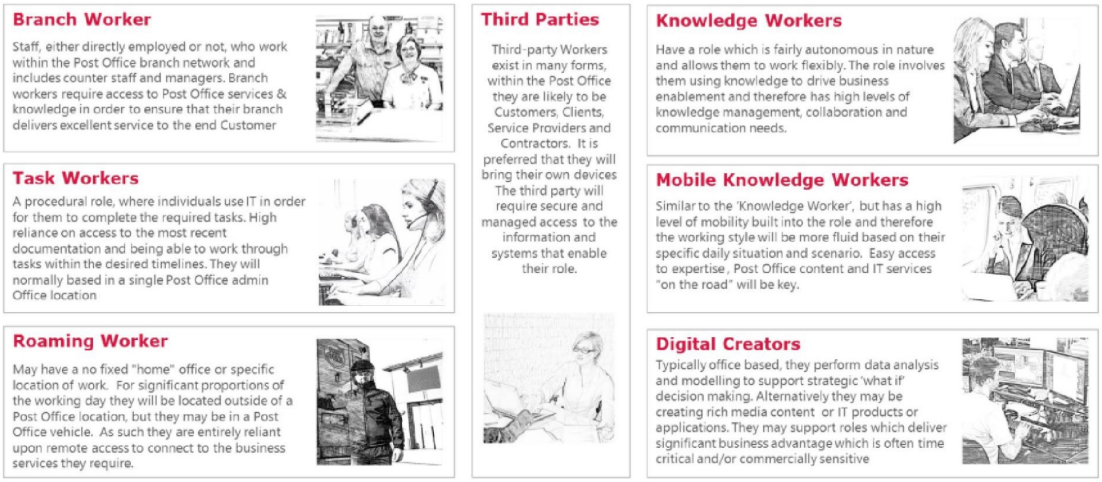


Figure 5: *Consumer types - Colleague IT services*

In terms of total numbers of each Persona, there are approximately:

- 990 Branch Workers
- 920 Knowledge Workers
- 880 Task Workers
- 380 Mobile Knowledge Workers
- 110 Roaming Workers
- 45 Digital Creators

3.3.1 Existing (As-Is) Colleague User Device Overview

The majority of the Colleague employees have one device allocated to them; however, some employees do not require continuous or regular access to a device and will utilise Kiosk mode devices primarily based in cash processing centres.

Of the circa **2650** existing devices, approximately 600 of these devices are desktops (Lenovo M79), and almost 90% of the remaining are laptops (Lenovo T440s), both of which are on average 5 years old. It is worth noting that all T440s devices have reached End of Service Life and supplies are no longer generally available.

There are a small proportion (c.200 devices) of users who have received a Windows Surface Pro as pilot devices and are utilising these for their day to day activities. This pilot introduced Windows 10 along with the new device hardware but did not include any service integration into the existing shared services used to underpin the estate (for example the devices therefore cannot utilise Follow Me Print, are not included on some security groups, etc). Details of the Windows 10 build can be found in the Technology Framework section 4.

The EUC estate for Colleagues also extends into the Branch network for the c.350 directly managed branches. The staff who work in these branches also have access to “back office” IT equipment in the form of either laptops & desktop to access the email system, all other employee IT systems and a print solution.

POL00337657

4. TECHNOLOGY FRAMEWORK

4.1 Technology Framework Overview

This Technology Framework section provides details of the technology used across Post Office and in-scope for the EUC Supplier. This framework represents the technology environment which will be managed by the EUC supplier under the EUC contract at the point of Implementation of EUC services. This Technology Framework will evolve over the lifetime of the EUC contract through agreed changes and change projects. Details of in-scope Transformational projects are provided in Section 10 of this Service Specification Document.

4.2 Shared Services

Shared Services refers to back-end infrastructure-based technologies and services that support the Branch and Colleague estates.

Shared Services infrastructure includes Microsoft Endpoint Manager (Intune), Active Directory and its associated technologies such as DNS and DHCP, SCCM and certificate services.

Currently, shared services are managed as a single unit of infrastructure that serves both the Branch and Colleague end user computing environment. This has previously caused a number of issues including where changes made in relation to the Colleague technologies have impacted the Branch environment and Postmasters ability to serve our customers. To minimise this, the new supplier will be required to work with Post Office to migrate Colleague to new and modern technologies where all devices and applications are managed and delivered through native cloud technologies. This will leave the existing Shared Services for the management of Branch counters and devices only (please see specific 'Shared Services Separation Project' requirements in Section 10).

The Post Office Limited is in the process of migrating the current on-prem EUC Infrastructure Shared Services to Azure IaaS Cloud Services and will have completed this migration prior to the award of the new EUC Services contract (see further details below).

The Shared Services technologies are shown in the below figure:

POL00337657

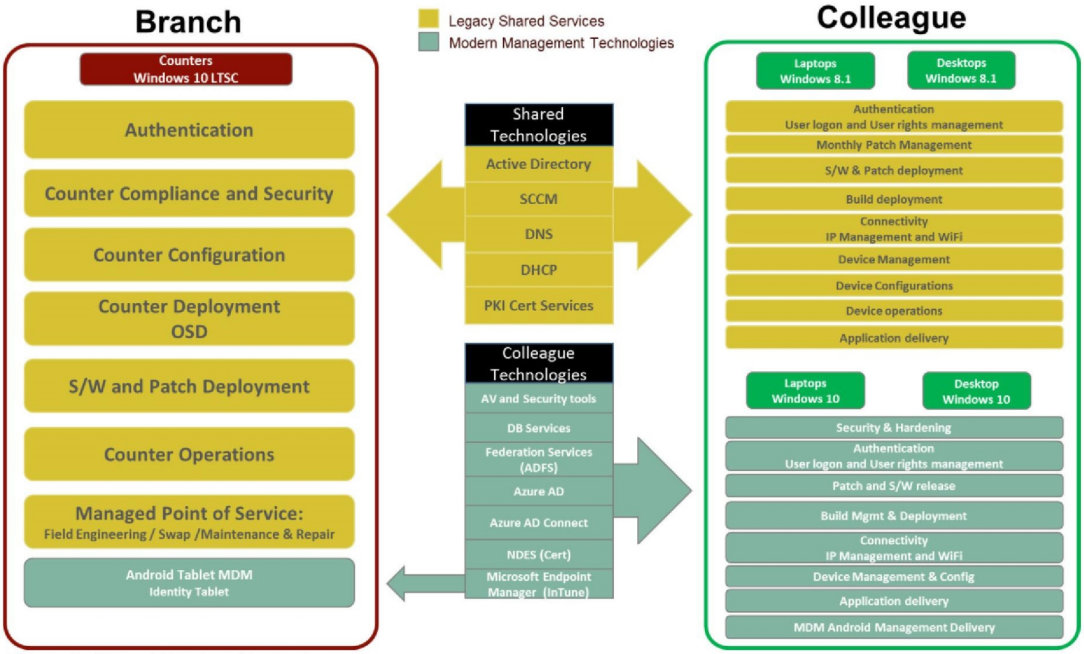


Figure 6: *Shared Services Technology*

4.2.1 Post Office Azure IaaS Cloud Services

The new Azure Platform benefits from a hub-spoke topology to provide scale with the ability to share key resources. Scale has been achieved by the additional spokes which share services in the hub to reduce cost and complexity. The hub-spoke topology is recognised as one of Microsoft's best practice models and is the topology of choice for Post Office's standard Landing Zone service.

This design is based on the foundation topology with the introduction of a second hub-spoke model within the UK's second region pair partner UK West, this is in addition to the UK South Region. This provides additional resilience for selective applications in the form of failover but strategically is used to architecture modern applications and provide load balancing and resilience across both regions.

The hub hosts the Azure Firewall and Domain Controllers as shared services with the former being used to control all traffic entering the hub from the spokes or externally as well as providing internet breakout. The placement of these services within the hub is in-line with Microsoft's reference architecture.

The Azure environment is connected via Microsoft's private circuit ExpressRoute and then onto the wide area network provided by Verizon that provides connectivity to the Post Office estate and partner locations.

Azure Log Analytics has been used for collecting and analysing logging and performance data from Azure resources such as Recovery Services Vaults, Key Vaults, VNets, Network Security Groups, Azure Firewall service and Virtual Machines.

Log Analytics has been deployed alongside ScienceLogic to collect logging data from supported Azure resources and Virtual Machines. A Log analytics workspace has deployed into the common services hub in each region and is used to collect logging data for resources within the same region, this will provide resiliency in the event of a region outage.

POL00337657

To protect and detect more advanced threats centrally in Post Office's Splunk SIEM solution, logs from critical Azure workloads and services are ingested in Splunk.

The Colleague and Shared Services technologies listed below are to be hosted in the Post Office Azure environment:

Services	Description	No of servers	Operating System
AD/DNS	Active Directory and DNS Services	6	Windows Server 2012 R2
AGMP	Advanced group policy management tool	1	Windows Server 2012 R2
Nessus	Vulnerability Scanning tool	2	Windows Server 2012 R2
Anti Virus	Symantec Endpoint Protection	3	Windows Server 2012 R2
Print	Post Office Managed Print services used in Colleague	7	Windows Server 2012 R2
MBAM	Microsoft BitLocker Administration and Monitoring	2	Windows Server 2012 R2
ADFS	Active Directory Federation Services	4	Windows Server 2012 R2
AAD Connect	Azure Active Directory Connect	1	Windows Server 2012 R2
Certificate	Certificate and NDES	3	Windows Server 2012 R2
Dell Active Roles	User and Group account management tool	2	Windows Server 2012 R2
Email Services	Exchange Hybrid Services including Mimecast	4	Windows Server 2012 R2
SCCM	System Centre Configuration Manager used for client management	7	Windows Server 2012 R2
IPAM	IP Management tool	1	Windows Server 2012 R2
PPE	Pre-Production Environment used for testing and pilot purposes.	48	SQL and Windows Server 2012 R2
SQL	Microsoft SQL servers used for EUC services	8	SQL

Table 4: *Shared Services Servers hosting in Azure*

The following diagram illustrates the new Azure IaaS environment where the above technologies services are to be hosted.

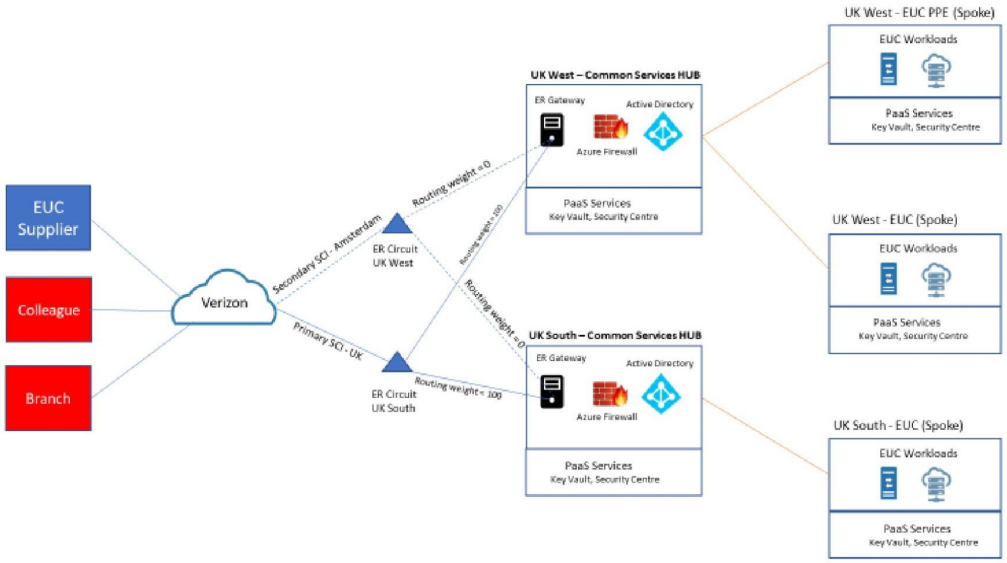


Figure 7: *Azure IaaS environment*

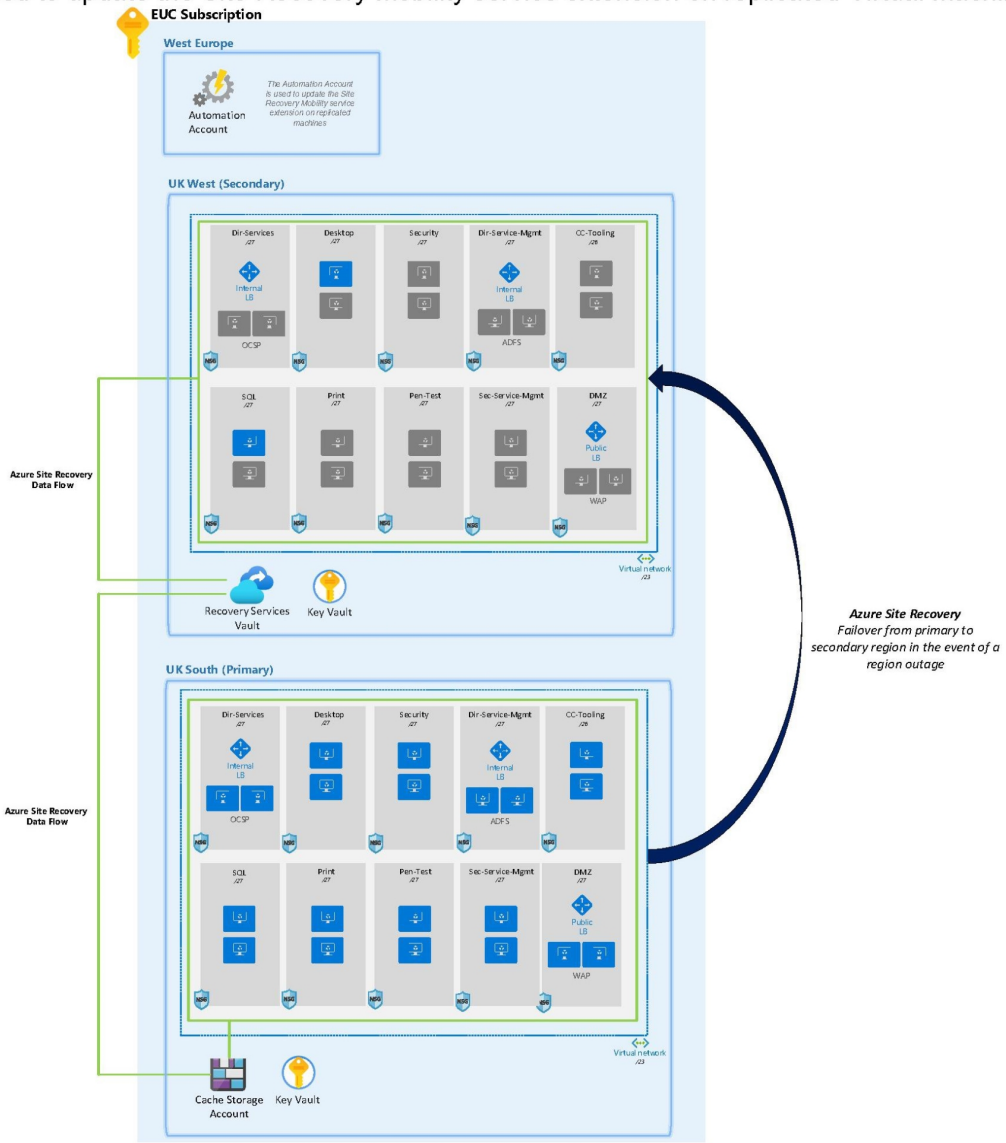
POL00337657

4.2.2 Disaster Recovery

The Azure Site Recovery service is used to replicate selected EUC workloads running on Azure Virtual Machines from the primary UK South Azure region to the secondary UK West region to provide redundancy in the event of a region outage.

The service protects workloads by replicating Virtual Machines from the source location to the target destination for Business Continuity and Disaster Recovery purposes. When an outage occurs at the primary location, a failover can be initiated to bring the workloads online in the target location by initiating a recovery plan to restore the latest recovery point and failed back when the primary region is available.

The following solution on a page illustrates the failover of EUC workloads from the primary Azure region to the secondary region using Azure Site Recovery. An Automation Account is used to update the Site Recovery Mobility service extension on replicated Virtual Machines.



POL00337657

Figure 8: Azure Site Recovery configuration

The below table provides a summary of in-scope Post Office EUC services for Azure Site Recovery.

No.	Service Name	Description
1	AD Group Policy Management	Hosts the Advanced Group Policy Management console used by support personnel
2	SCCM	Configuration Management tool providing Patching, Software Distribution & Build for Post Office Colleague clients and Branch counter devices
3	ADFS incl. AD Sync	Providing single sign on for cloud applications including Office 365. AD Connect provides directory synchronisation between Windows Active Directory and Azure Active Directory
4	MBAM	Providing BitLocker Administration and Monitoring services for encrypted devices on Post Office Colleague clients and Branch counter devices
5	Certificate incl. NDES	Supplier's public key infrastructure (PKI) providing public key cryptography, digital certificates, and digital signature capabilities for EUC services. Network Device Enrolment Services (NDES) allows the Intune managed mobile devices to obtain SCEP certificates from the CA
6	SQL Server	Hosting database and reporting services for selective services
9	Managed Print (print server infrastructure only)	Providing 'follow-me' printing facilities for Post Office Colleague clients. Azure Site Recovery for the print servers, Managed Print software is the scope of Managed Print Supplier.
10	Email Services incl. MIME	Provides secure mail routing between on-premises and Exchange Online

Table 5: *In-scope Post Office EUC services for Azure Site Recovery*

Active Directory Domain Controllers, DNS and Symantec Endpoint Protection services are not included in Azure Site Recovery configuration. These services are designed and implemented in an Active/Active setup, providing high availability services that run in both Azure regions.

Note: With the migration of EUC infrastructure to the Post Office Azure environment Post Office is reviewing the BCDR/ITSC Plans and Policies, including Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) for the EUC Services. These documents will be provided to the EUC Supplier at contract signature to input in to the required EUC Supplier Disaster Recovery Plan.

POL00337657

4.2.3 Server Build

The standard operating system used on all Post Office servers is Windows 2012 R2 that is designed and delivered through Microsoft Azure Image Builder. This technology is used to create standardised build images for Virtual Machines and Shared Image Gallery which provides image storage, management and distribution functionality.

The Azure Image Builder related resources are deployed into a single Resource Group within the Post Office EUC subscription located in the UK South Azure Region.

Images are built in the West Europe region and are distributed to UK South and UK West regions for consumption.

A Storage Account is created to store build artefacts such as applications and scripts that are downloaded to the build image during the customisation process.

The Azure Image Builder Service uses a Managed Identity to access Azure resources such as the Shared Image Gallery and build artefact storage account.

Monthly patches and security updates are all reviewed and deployed using SCCM on all servers.

The servers are all located in their dedicated OUs in Active Directory, where organisation wide configurations are applied using Group Policy Objects. This includes security configurations and customisations.

4.2.4 Active Directory

Post Office's Active Directory Forest is setup based on Microsoft's best practices with a sub Domain name of postoffice.co.uk. The sub Domain name for this forest is euc.postoffice.co.uk. The legacy NetBIOS name is EUC.

The forest functional level is set to Windows Server 2012 R2. Only Windows Server 2012 R2 Domain Controllers are currently supported at this level.

The Domain functional level of 2012 R2 includes the following features:

- Kerberos armouring.
- DC-side protection for Protected Users.
- Authentication Policies.
- Authentication Policy Silos.

Two Domain Controllers are deployed in each region (UK South and West) within each hub. The two production spokes participate in their region hubs Windows Domain via the VNet Peer.

All Domain Controllers in the Domain are configured as Global Catalogue servers without any functional or performance penalty.

Directory site is configured to host all other subnets not specifically included in an Active Directory site.

4.2.5 DNS

POL00337657

Post Office has a registered DNS Domain name of postoffice.co.uk. The name is used externally as the suffix for employee's e-mail addresses and for web presence. A sub Domain of EUC prefixes the registered name to separate internal and external name spaces.

All Domain Controllers host the DNS service and all zones are AD integrated. Configuration of DNS is standardised across the DNS servers with the exception of a designated server that is configured for DNS scavenging.

4.2.6 DHCP (out of scope for EUC contract)

The DHCP servers dynamically assign an IP address and other network configuration parameters to each device on the network, so they can communicate with other IP devices. An example of this is the that all Colleague devices such as desktops and laptops receive their DNS servers IP addresses from the DHCP servers.

DHCP is used in Branch during build deployment only. Counters are setup to use static IP addresses. Colleague user devices are fully dependent on DHCP. Currently Lease is set to 8 hours when the clients request IP renewal every 4 hours.

Historically, DHCP services have been provided from the current EUC Supplier's datacentres. Since DHCP services cannot be delivered from MS Azure, Post Office are in the process of migrating DHCP services to the current Networks service supplier who will be delivering DHCP services from their datacentres. The EUC supplier will need to work with the Networks supplier to ensure that all in scope clients are using optimal DHCP configurations. This includes the ongoing management and configuration of DHCP on all Colleague clients and Branch counters, where applicable.

4.2.7 Config Manager (SCCM)

Config Manager provides systems management facilities for both Windows clients and Windows servers operating within the Post Office environment. The current SCCM design is based on a single primary site implementation of Config Manager that can be scaled up to support a maximum of 100,000 clients.

The functionality of the solution includes additional products such as:

- The Microsoft Deployment Toolkit (MDT). This provides OS deployment capabilities.
- 1E Nomad. This provides a peer-to-peer content distribution mechanism.

The server infrastructure, that forms the operational core of the solution, is centralised in Azure and resides within the EUC.POSTOFFICE.CO.UK Active Directory domain. All managed clients are located within this domain. The Config Manager solution is hosted in Azure UK South and includes duplication for some of the critical server roles to ensure a high level of fault tolerance is achieved.

The solution delivers the following systems management facilities within the Post Office environment:

- Desktop and Server Management.
- Windows 8.1 deployment for both Colleague and Branch devices and users.
- Software distribution (MSI & App-V).
- Hardware & Software Inventory.
- Patch management for Windows products.
- Helpdesk remote support to devices in the Colleague departments Device management.

POL00337657

4.2.8 Certificate Services

An internal Certificate Authority is available that essentially provides a private base certificate which can issue other private certificates for internal servers and users. Common uses of Private CA's include:

- Intranet Sites.
- Device identification.
- VPN.
- Securing communications between internal sites.

Additionally, as part of modern management, in conjunction with Microsoft Endpoint Manager, an NDES server is used to manage Certificate enrolment using SCEP (Simple Certificate Enrolment Protocol) profiles to deploy, retire and revoke certificates.

4.2.9 Microsoft Endpoint Manager (Intune)

Microsoft Endpoint Manager services provide access to corporate data through device and application management controls to corporate and non-corporate devices.

At Post Office Microsoft Endpoint Manager is used for the management and delivery of:

- Compliance policies.
- Device enrolment.
- Enterprise deployment profiles (Android and Windows 10 Autopilot).
- Application deployment and protection.
- BYOD policies.
- Conditional access.
- Microsoft Defender ATP.
- Device health reports.

Windows Devices:

- Autopilot Windows 10 Colleague build and its ongoing management.
- Currently 200 pilot devices deployed.

Mobile Devices build and device management:

- Colleague mobile devices (Out of scope of EUC contract).
- 20 Colleague Pilot CViT Android.
- 800 Branch Android tablets for identity services.

4.3 Branch Technologies

The EUC Branch technology environment is comprised of:

- Branch Point of Sale (POS) technology devices (base unit, keyboards, scanners, monitors, receipt/label printers).
- Infrastructure Technology (Datacentre/Azure hosting, compute, system management, identity, security solutions, application delivery etc).
- Shared Technology (Active Directory, Domain Name Services, Print Management, Anti-virus, device certificate management etc) used to under pin and facilitate delivery of Branch technology (note this is currently shared with Colleague).

4.3.1 Branch Devices

POL00337657

Branches have a base set of technology (with some variation of actual equipment) that enable the provision of core services (mails, banking, billpay). In addition to the base set of technology, some branches also have additional technology to enable further services, or ways of working (e.g. Self-Service Kiosks - SSKs).

There is also variation in technology depending upon the type of Branch (e.g. Outreach/mobile sites have variations to allow mobile working).

As part of a Branch refresh programme the below counter hardware models were deployed:
Phase 1 roll-out (c.8000 counters) based around M79 build
Phase 2 roll-out (c.15000 counters) based around PX35 build

The table below highlights the setup of the counter models and their corresponding peripherals:

Item	Required per counter M79	Required per counter PX35	Required per Branch M79	Required per Branch PX35
Lenovo M79	1			
PX35		1		
PX35 Red Cable used on Pinpads - 100%		1		
PX35 Blue Cable used on Scales- 100%		1		
PX35 Green Cable used on devices with Rateboards (50%)		0.5		
Epson Printer	1	1		
Epson Cartridge	1	1		
Barcode Scanner with cable	1	1		
RJ12 to serial for M79	2			
USB A-B 2mtr	1		1	
USB A-B 4Mtr				1
USB A-B 5Mtr - if 4mtr not available				
Coupler - Direct to BB		1		
Ethernet extension 2mtr - Direct to BB		1		
15' monitor	1			
Tipro keyboard	1	1		
Canon printer				1
Serial to USB - M79 Rate Board	0.5			

Table 6: *Counter Setup Devices*

The following table provides an overview of all branch devices, including peripherals:

Device Name	Description	Branch Type	Supplier Scope
Branch Till	Till used at counters to process Customer transactions. These include: • Base unit (BoxTech Cielo tablet or Lenovo M79 / PX-35). • The till operating system is “kiosk” version of Windows which is Windows 10 LTSC • Bar Code Scanner. • Multifunction printer (Receipts and Labels) - Epson TM7200 – Designed for Post Office	All	Yes

POL00337657

	• Specialised Keyboard = Tipro Keyboard - TIP-002-999 • Electronic Scales (may be shared at 2:1 ratio). • Pin Entry Device (Ingenico IPP350). • Scales Connector (shared between counters).		
AEI	• KVM Switch for AEI devices (shared keyboard).	Some branches (1000)	Yes
Identity Tablets	• Android Identity Tablets managed by MS Endpoint Manager (Intune) This includes Device Management, App Management, Security Management, Content Management, Email Management and Containerisation.	Currently 800 Devices	Yes
PayStation	PayStations enable Customer to make bill payments. These devices are independent of the branch counter, using their own separated comms links. PayStations are managed directly by Paystation, an arrangement which falls under the Branch Network Business department in Post Office.	DMB, Main & Local	No
Backoffice Counters	A Backoffice counter that is used for management processes, balancing and stock ordering.	Some Branches	Yes
Backoffice Printer	Canon A4 printer used for account balancing and report purposes.	All Branches	Yes
Safe	Used in branches to store cash and valuables.	DMB, Main & Local	No
Alarm System / CCTV	Branch burglar alarms and CCTV surveillance systems.	DMB, Main & Local	No
Anti-robbery fogging system	Anti-burglary fogging system installed and maintained by third party supplier in 2000 high risk branches.	All High-Risk Branches	No
Branch Router	ADSL routers provided by Verizon as part of branch networking service. Some routers provide branch Wi-Fi.	DMB, Main & Local	No
Branch network circuit	Branches connected via either ADSL, Mobile or VSAT network connections. Where possible the mobile network is used as a redundancy solution.	DMB, Main Local, & Outreach	No
8 Port Hubs	Hubs providing internal network connectivity for branch connected devices.	Some branches	Yes

Table 7: *Overview of Branch Devices*

4.3.2 Peripherals

The peripherals used in Branch vary a great deal depending on the branch type which determines the service which are offered to Customers. The following table summarises the

POL00337657

set of peripherals used in Post Office branches which fall within the supplier management scope:

Peripheral	Description
Bar Code Scanner	Bar code scanner used with Branch Counter to scan product details.
Epson Printer	A multifunctional printer used with Branch Counter to print postage labels, Customer receipts and secure items such as Postal Orders.
Counter Keyboard	A specialised robust keyboard used with Branch Counter.
Cash Drawer	A secure cash drawer that is not activated by the Branch Counter.
Scale Connector	Connection between Postage scales and the Branch Counter to weigh letters and parcels to determine postage rates.
Pin Entry Device	An Ingenico IPP350 pin pad used with Branch Counter to verify Customer card PINs.
Magnetic Stripe Reader	A magnetic stripe reader used for gift cards and bill payments.

Table 8: *Overview of Branch Peripherals*

4.3.3 Cabling

The supplier is responsible for managing the cabling in branches, and this includes network cabling, KVM switches (used for the AEI identity terminals) and other device cabling e.g. power supplies and port connector cables.

The supplier should organise/ reorganise branch cabling to ensure that cabling is managed in an ordered way, cables are labelled in terms of their use, and through the use of colour coding to facilitate supplier engineers and remotely assist branches to self-serve.

4.3.4 Branch Network

Branches use a variety of network setups in order to provide connectivity between branches and the central Post Office services.

The network type used in branches is related to the size of the branch. Network types include ADSL, mobile 4G connections and Very Small Aperture Terminal (VSAT). Branches use private networks which reduces the vulnerability to outside attacks.

The branch circuits, circuit terminating equipment, and network devices (such as switches and Wi-Fi routers) are managed by Verizon Networks which makes use of a number of Talk Talk ADSL circuits.

The following is a branch network architecture diagram used to illustrate the branches networks, comms links and network devices in relation to the wider Post Office networks.

POL00337657

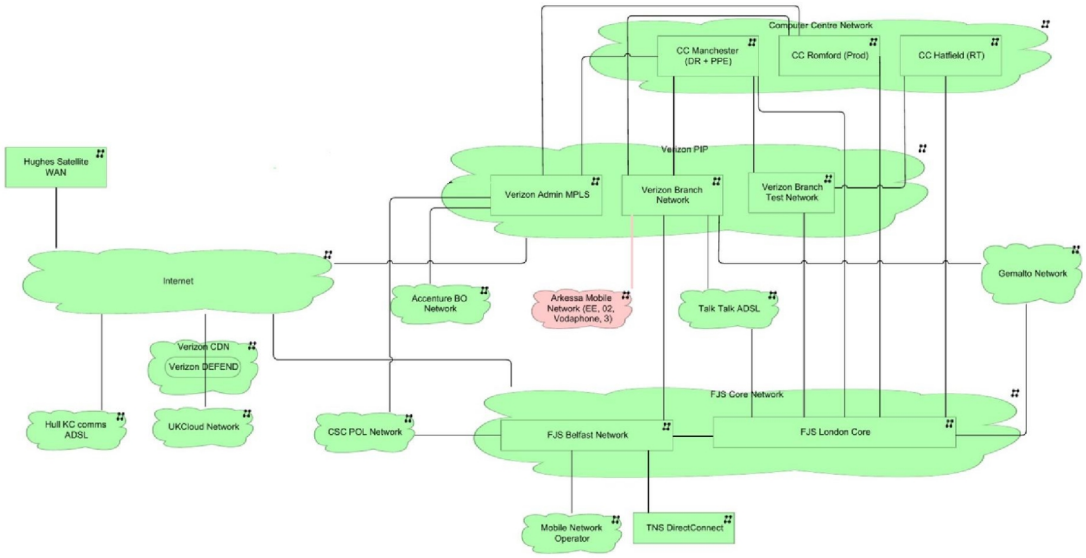


Figure 9: *Branch networks, comms links and network devices*

4.3.5 Counter Application Delivery

The Horizon Next Generation Application (HNGA) is the application used by Postmasters in every Post Office branch when serving Customers. Although the Postmaster only ever sees one GUI (Graphical User Interface), HNGA is not a single application, it is actually made up of a suite of individual applications including runtime utilities such Java and Microsoft Visual C.

Note that it is possible that the number of applications that make up HNGA may increase or decrease over time.

The HNGA supplier develops the HNGA application for the Post Office and whenever they release a new version, one or more of the above components may change to a newer version.

When a new version of HNGA or its components are available, the EUC supplier will need to update the existing HNGA package in SCCM and arrange for its deployment in production.

As part of the deployment the EUC supplier will need to adhere to Post Office's change & release management processes & policies and arrange for the necessary tests which should be completed in the Pre-Production Environment (see below) and if necessary, on physical counter devices, before the new application is released for UAT and Pilot testing.

4.4 Test and Release

All software releases and patch updates are fully tested by the EUC and Counter Software suppliers and validated by Post Office before they are released into the production environment.

The EUC Supplier manages the hardware and the operating system core build which runs the Branch counter application provided by another Third-Party Supplier. For the Branch counter application to operate successfully, additional reference data is used to support the

POL00337657

configuration, which is controlled and maintained by Post Office. For any changes to the hardware or software, at any level, consideration and End-to-End testing needs to be coordinated across the relevant parties and test environments.

The following environments are used for test and validation purposes.

4.4.1 EUC Pre-Production Environment (PPE)

An EUC PPE environment is available for staging and testing purposes that resembles Post Office's EUC production environment. The primary use of this environment is to perform the initial test for all installation/configuration/migration/patching/OS build updates activities and procedures before they're deployed in the Production environments. This ensures all major and minor upgrades to a production environment are completed reliably, without errors, and in a minimum of time.

The PPE is configured to mirror our actual production environment as closely as possible for testing of key applications such as Horizon and the supporting technologies such as SCCM, OS Builds and Active Directory.

The PPE environment is hosted in the Azure UK West region (Shown in Figure 7) which consists of 38 Servers providing key EUC technologies such as Active Directory, DNS, PKI, SCCM, SEP, SQL, ADFS and Exchange Hybrid. Additionally, there are 6 virtual desktops used for core build and application testing purposes.

Post Office requires the EUC supplier to fully manage the PPE platform which should mirror the production environment.

4.4.2 Solution Validation and Integration (SV&I) - 3rd Party Environment used by Post Office

The second environment used during the test and validation process is SV&I. This environment is used to provide test assurance of any IT changes undertaken on the Horizon Point of Sale system which has connectivity to the many Third-Party client test systems and allows us to perform End To End (E2E) testing in a realistic manner. Integration testing when changes span multiple systems is also undertaken on this environment. The bulk of Horizon changes are implemented via reference data, however the remainder of changes are through APADC scripting or core Horizon code changes.

The EUC Supplier will provide break fix support for the SV&I hardware and peripherals which comprises of Branch counter positions which are only connected to test environments.

- 28 counter positions, each with a mixture of peripherals (e.g. PIN pads, barcode scanner, counter printer, back office printer, weigh-scales, FOREX rate-board etc).
- SV&I Kit located at Finsbury Dials and Future Walk.
- 3 home deployed counters.
- Types of testing undertaken on the kit:
  - Functional testing of significant Reference Data changes – i.e. introduction of new products/services.
  - E2E testing with external 3rd parties.
  - Branch Counter Regression testing when other integrated systems change, including network and infrastructure changes.
  - Regulatory changes (e.g. PCI, GDPR).
  - System Accreditation / Certification testing.

POL00337657

- Support Post Office UAT.
- Functional testing includes:
    - Current production defects retrofits
    - Inherited defects
    - Landscape Defects
    - Core regression
    - End to End testing

4.4.3 LST – Live System Test (3rd Party Environment)

This environment consists of physical counters which are used and managed by the Third-Party counter software supplier to prove deployment and support processes prior to change deployment in production. This environment is exclusively owned and operated by the software supplier. When required, independent penetration testing of the counter software solution is performed on this environment.

The EUC Supplier will provide break fix support for the LST hardware and peripherals which comprises of Branch counter positions which are only connected to test environments.

4.4.4 Reference Data Test (RDT) Customer Environment

This environment is used to develop, maintain and verify reference data, and for small simple changes. For complex reference data changes, or changes that span multiple systems, this is undertaken on the SV&I environment providing independent test assurance. Upon request, the test team also support to the Post Office running User Acceptance Testing (UAT) to verify changes from a user perspective.

- 13 counter positions with a mixture of peripherals (e.g. PIN pads, barcode scanner, counter printer, back office printer, weigh-scales, FOREX rate-board etc).
- 3 home deployed counters.
- Kit located at Finsbury Dials and Future Walk.
- Types of testing undertaken on the kit:
    - Reference Data Development, Unit Testing and Verification

The EUC Supplier will provide break fix for the Reference Data Rigs hardware and peripherals which comprises of Branch counter positions which are only connected to test environments.

4.4.5 Model Office – Customer Live Environment

The final part of the test is to deploy all releases to the Model Office counters. This consists of 7 counter positions which can be set up to reflect 5 different type of live branches, so we are able to demonstrate any transaction, providing a real-time experience the same as that which our Postmasters would see in their branches.

Model Office has the same technology as you would expect to see throughout our network including Horizon kit, barcode scanners, counter printers, back office printers, PIN pads, Self Service Kiosks, AEI, Cash Deposit Machine, Paystations etc.

Upon confirmation of successful deployment, the Supplier arranges for the production deployment.

POL00337657

The above process is illustrated in the Counter Patch Management diagram provided below in figure 10.

4.4.6 Configuration Baseline and Compliance

Post Office requires that branch counters are always kept compliant for a specific version of HNGA. The counters must not be allowed to run unless they are compliant with the correct version of HNGA.

Each release of HNGA must have its own Configuration Baseline configured in SCCM which is then deployed to a base device collection. This allows easy targeting of the Baseline by using Include Collection rules to target the baseline at collections of devices. Each baseline is made up of a single Configuration Item that contains 12 registry checks, one for each of the component applications that make up the HNGA suite.

During the build, a version of HNGA is installed, and then at the end of the build, Build Stage compliance AD groups and Collection memberships are used to set the HNGA baseline version that the counter needs to be compliant to. At the end of the Task Sequence stage of the build a set of PowerShell scripts will execute which will test the counters compliance to the designated HNGA baseline. If the counter is Non-Compliant, it will go through the standard process to become Compliant, and when the counter is confirmed as Compliant the build will complete successfully.

The EUC supplier is responsible for the implementation of the SCCM Configuration Baselines to ensure that HNGA is kept at the correct version on every branch counter. It is accepted that there will be different versions deployed in the estate as part of test and pilot activities and during upgrade periods.

4.4.7 Branch Counter Design

Windows 10 Enterprise 2016 LTSB x64 build is deployed to the counter devices through the OS deployment features provided by the SCCM solution. The deployed counter devices run the HNGA applications and are managed by the systems management infrastructure technologies.

All devices are deployed as new devices. No data or state information is migrated from existing legacy point of sale system (LPOSS) counters to new modern point of sale system (MPOSS) counters.

Windows 10 Enterprise 2016 LTSB x64 volume license media is stored within SCCM to form the basis of the deployed builds.

The build is installed on production and non-production counter PCs at the current Supplier's DC Configuration Centre. These counter PCs use the generic builds, in advance of their deployment and personalisation as a counter within a Post Office branch. Two physical SCCM servers are installed in the current EUC Supplier's Configuration Centre to support a concurrent build volume of up to 160 devices. The use of shift patterns caters for up to 200 deployments per day.

The latest operating system updates that have been tested and approved for use with the build HNGA are then installed during the deployment process.

Once delivered to site, the counter PCs are installed for the particular branch and counter node position in order to comply with financial audit requirements. This process is referred to as "personalisation" and is performed by the deployment Engineer using a custom script developed by the current EUC supplier known as the "Counter Deployment Utility" (CDU). The CDU prompts the Deployment Engineer for a number of parameters for the particular branch and counter instance and communicates with the Horizon software supplier Services

POL00337657

data centre to retrieve configuration parameters. When the CDU finishes and personalisation is complete the counter client is locked down.

4.4.8 Counter Anti-Virus – Windows Defender

Microsoft Windows Defender is part of the default Windows 10 installation that provides protection against viruses or other malware that may have infiltrated the computer. Windows Defender is retained as the standard anti-virus and malware protection product on Branch Counter Windows 10 devices and is centrally managed and updated using SCCM.

4.4.9 Counter Patch Management

The build is patched centrally as part of the EUC Supplier's patch management service. The patch management process and associated testing must be carried out in line with PCI requirements.
The patches and updates are currently delivered and installed by the SCCM infrastructure, and 1e Nomad which has been installed to improve SCCM content download.
The EUC Supplier uses SCCM and 1e to deploy monthly patches to all Windows 10 LTSB counters. As part of this activity the supplier performs:

- Discovery – Ensure there is a comprehensive inventory of all end point devices.
- Monitor for new patches and vulnerabilities - Understand MS patch release schedules and perform vulnerability assessment. Where possible, only install the necessary patches.
- Patch testing – Use the PPE/Testing environment to avoid being caught off guard by unintended issues.
- Configuration management - Document any changes about to be made via patching.
- Patch release – Follow patch deployment procedures.
- Auditing - Conduct a patch management audit to identify any failed or pending patches and continue monitoring for any unexpected incompatibility or performance issues.
- Repair - Proactive deployment remediation on counters where deployments have failed.
- Reporting - Produce a patch compliance report.
- Review, improve and repeat - Establish a cadence for repeating and optimising the above steps.

POL00337657

The below figure shows the processes required to complete patch deployment on counters:

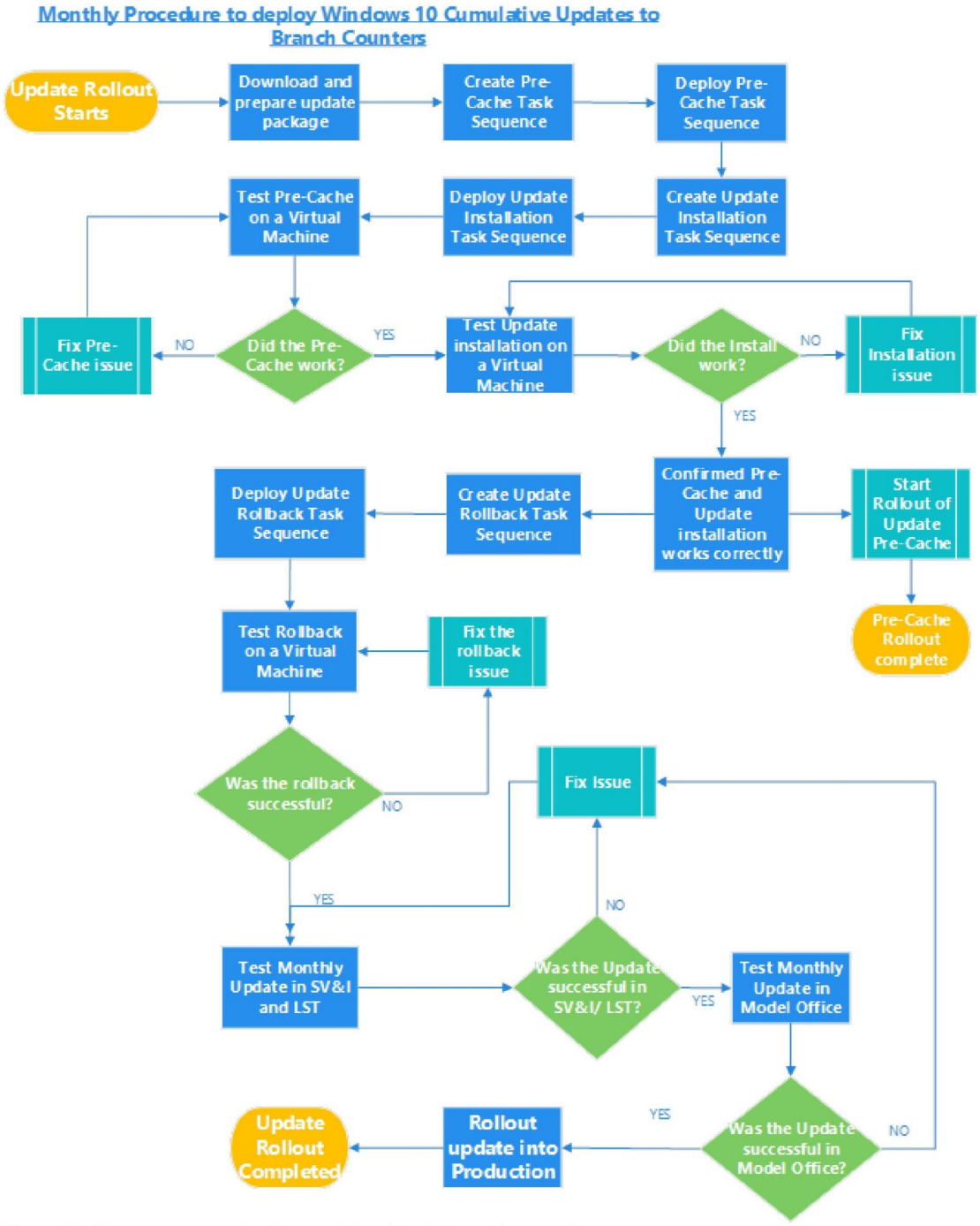


Figure 10: *The processes required to complete patch deployment on counters*

.

POL00337657

4.5 Colleague Technologies

The EUC Colleague technology environment is comprised of:

- Windows 8.1 on Lenovo laptops & Desktops – Managed using Microsoft System Centre Config Manager (SCCM).
- Pilot Windows 10 on MS Surface Pro tablets – Managed using Microsoft Endpoint Manager (Intune).
- Standard Core build applications and utilities.
- Office 365 and Email Services including Anti-Spam and Anti-Phishing.
- Supplier's SubCA Certificate Services.
- Federation Services.
- Anti Virus Services.
- Infrastructure Technology (Datacentre/Azure hosting, compute, system management, identity, security solutions, application delivery etc).
- Shared Technology (Active Directory, Domain Name Services, Print Management, Anti-virus, device certificate management etc) used to underpin and facilitate delivery of Colleague technology (note this is currently shared with Branch devices).
- Device supply and repair.
- Application Delivery.

4.5.1 Colleague Devices

The majority of the Colleague employees have at least one device allocated to them; however, some employees do not require continuous or regular access to a device and will utilise Kiosk mode devices primarily based in cash processing centres.

The below table provides an overview of Colleague devices:

Device	Models	Numbers	Operating System
Main Desktops	M79 SFF	591	Windows 8.1
Additional Desktops	M79, M910, P510	8	Windows 8.1
	Desktops Total	***599***	
Main Laptops	Thinkpad T440s	1659	Windows 8.1
Additional Laptops	T440, T450, T450s, T460s, T540p, T560, T570	200	Windows 8.1
	Laptops Total	***1859***	
Tablet (Pilot)	Surface Pro 7	200	Windows 10
	Tablets Total	*200*	
	Devices Total	**2658**	

Table 9: *Colleague Devices*

In addition to the above managed devices, the supplier will need to support a small number of Post Office owned Apple devices for VIP users who are Post Office executives. The supplier will need to provide warranty repair or replacement, end-user support and asset management.

The EUC Supplier should note that **Post Office do not require options for 'Device as a Service' solutions.** The scope of the EUC Contract services requires the EUC supplier to deliver the device management /managed device services only.

4.5.2 Windows 8.1

POL00337657

Post Office has 1859 laptops and 599 desktops with Windows 8.1 as an operating system with 200 Microsoft Surface Pros operating on Windows 10.

The standard operating system used on End User devices is Windows 8.1. A Zero Touch Windows 8.1 MDT build has been created using SCCM that can be deployed to all supported End User devices. This build includes standard core applications and utilities such as:

- Hardware drivers and utilities including attached printer drivers and drivers for the FollowYou printers.
- MS Office 365 Apps for Enterprise.
- SEP AV.
- Adobe Reader.
- Cisco AnyConnect VPN Client.
- 1E Nomad.
- Eracent (Asset Management tool required, deployed and fully managed by the current EUC supplier).
- MDOP MBAM.
- MS Visual C++.
- Post Office Screen Saver.
- Device and user Certificates.
- Corporate fonts.
- Custom desktop and wallpaper.

A full list of packaged software applications is provided in **Appendix A: Ref Doc-004 POL Device Software.**

The build is managed through SCCM and is updated twice a year unless there is a requirement for a major change.

The Colleague build core applications, drivers and utilities are updated on a request basis. Most of the drivers and utilities have not been updated since the first major build release in 2015.

All devices are AD/AAD hybrid joined and are configured using AD Group Policy Objects. OS and Application specific GPOs are linked to the OUs where the devices and user account objects are located.

4.5.3 Application Delivery

All applications are packaged in MSI format and deployed through SCCM to the end point devices. Requests for new application packages or existing ones are created in the corporate ITSM tool. This process also includes asset and license management activities to ensure compliancy.

4.5.4 Patch Management

All Builds including the desktop and laptop contain the agreed patches to protect against known security vulnerabilities and any further patches reasonably required.
As part of this service Monthly Microsoft Quality Updates and Microsoft Security Updates (aka security Patch Tuesday) are deployed in the estate based on an agreed patch deployment schedule. The schedule includes deployments in Test, Pre-Production & Pilot environments before they are deployed in production.

4.5.5 Anti-Virus

POL00337657

The Anti-Virus solution currently deployed within the Post Office's Windows 8.1 estate is Symantec Endpoint Protection.

The SEP Suite consists of the following components:

- Live Update Server (LU).
- Symantec Endpoint Protection Manager (SEPM).
- Symantec Endpoint Protection Agent (SEP).
- Shared In-Sight Cache (SIC).
- Symantec Endpoint Protection Engine (SPE).
- Database, using Microsoft SQL Server

The current SEP solution runs SEP 12.1 and runs only from the UK South Azure environment. Resilience is provided by a replicated SQL cluster that has instances in both UK South and West.

In normal operations all SEP Clients will talk to the 2 SEPM servers in the UK South Azure environment. In a DR scenario, all SEP Clients will automatically switch to communicate with the 2 SEPM servers in the UK West Azure.

4.5.6 Windows 10 Pilot

To prepare for the target state, an Autopilot Modern Management Windows 10 build has been created to pilot the migration of all devices & apps from Windows 8.1 to Windows 10. Currently there are 200 Windows 10 Surface Pro devices that are Azure AD joined and are enrolled within Microsoft Endpoint Manager to enable the functionality for Post Office to control the devices configuration and apply restrictions.

4.5.7 Windows 10 Design

This build is designed based on Windows 10 Autopilot where the serial number of the approved corporate devices are managed within Microsoft Endpoint Manager portal. The build is Azure AD integrated where all Windows 10 devices are AAD joined and authentication is achieved through AAD user IDs.

Applications are packaged and delivered through Microsoft Endpoint Manager to Company Portal to the users. Additionally, Microsoft Endpoint Manager Application protection is configured to help protect Post Office company data, by using Microsoft Endpoint Manager Application Protection policies that will control the use of managed applications with the use of the user's corporate credentials.

Windows 10 build includes standard core applications and utilities such as:

- Hardware drivers and utilities.
- MS Office 365 Apps for Enterprise including Teams.
- Cisco AnyConnect VPN Client.
- Microsoft Edge.
- MS Visual C++.
- Post Office Screen Saver and branding.
- Microsoft Defender ATP.
- Bitlocker encryption.
- Zscaler Client Connector - Forwards user traffic to the Zscaler cloud and ensures that security and access policies are enforced. This solution should be reviewed as part of the Windows 10 Upgrade project highlighted in the Transformation section.

POL00337657

The Windows 10 Autopilot allows for the build deployment and customisation to be completed in a self-service manner by the users remotely or in the office.

During the build deployment, the customisation process that is developed and deployed through Microsoft Endpoint Manager, will configure the devices with security and features required by Post Office. This includes implementing all security policies, branding, installing core build applications, utilities and publishing user applications in company portal.

4.5.8 Application Delivery

All applications are packaged and deployed through Microsoft Endpoint Manager and delivered to the users in Company Portal in a self-service manner. Requests for new application packages or existing ones are created in the corporate ITSM tool (ServiceNow – See Section 8 for details). This process also includes asset and license management activities to ensure compliancy.

4.5.9 Patch Management

Windows 10 devices are kept up to date with all Quality updates to protect against known security vulnerabilities and any further patches reasonably required.

As part of this service all Monthly Quality Updates (every security Patch Tuesday) are deployed in the estate based on an agreed patch deployment schedule. The schedule includes deployments in Test, Pre-Production & Pilot environments before they are deployed in production.

Windows 10 Feature Updates and device drivers are reviewed and assessed in collaboration with Post Office's IT and security teams before they are deployed to the clients.

4.5.10 Windows 10 DR Build

Post Office is in the process of creating an Autopilot Win10 DR profile with a set of standard DR applications to provide the key users with equipment in the event of loss of access to Post Office sites. This solution negates the requirements for having dedicated recovery sites and office spaces for the DR plans. This solution will provide circa 120 DR laptops.

4.5.11 Office 365

The Post Office transitioned away from the traditional volume licensing approach for Microsoft Office to subscription-based licensing model in 2019. To be compliant, Office 365 1908.11929 (Semi-Annual Enterprise Channel) has been installed on all Colleague Windows 10 and Windows 8.1 devices. This includes apps such as MS Word, PowerPoint, Excel, Outlook and Onedrive.

All Office 365 apps and services are connected, both to each other and to the wider web, facilitating teamwork, saving employees time and enabling them to work better together through tools such as Teams chat, online meetings, co-authoring and sharing files, and group emails. The inclusion of cloud storage and mobile apps in the Office 365 suite also allows the colleagues to work wherever, whenever, with secure access to content, conversations, tasks, and schedules.

The Post Office owns and is responsible for the licensing of Microsoft 365 Apps. The Supplier is responsible for the management, packaging and deployment of all 365 & Enterprise apps including productivity and collaboration suite of applications.

POL00337657

SCCM is used to download the required Microsoft 365 Apps for Enterprise source components, using the in-built Microsoft 365 Apps for Enterprise Client Management functionality. It is also used to deploy the Microsoft 365 Apps for Enterprise client applications using the download and execute model, in association with 1E Nomad.

Group Policy Objects in Active Directory are used to configure all MS Office applications on Windows 8.1. devices.

Microsoft Endpoint Manager has been used to deploy using the download and execute model and manage Microsoft 365 Apps on all Windows 10 devices. This includes the deployment of monthly patches. This also includes all configurations and security settings.

Applications which require additional licences e.g. Visio and Project, are managed separately to ensure licence number compliance and installed versions are deployed via SCCM and Microsoft Endpoint Manager.

4.5.12 Email Services

Post Office uses Office 365 to manage all workflows including the management of mailboxes and filtering.

The Microsoft Outlook client version 1908.11929, included in the licensed version of Office 365, is installed and configured on End User Devices to connect to Office 365 for emails and other tools such as calendar appointments, tasks, contacts, and notes. User mailboxes are configured to run in cache mode allowing users to work offline when needed.

Post Office also has 2 On-prem Exchange 2013 CU23 Hybrid servers (with the latest patch releases) to allow secure mail routing between on-premises and Exchange Online. The Hybrid servers also provide SMTP relay for applications which are unable to relay via Office 365.

4.5.13 Federation Services and Identity synchronisation

Post Office has Active Directory (AD), Azure Active Directory Connect (AADC) and Active Directory Federation Services (ADFS) infrastructure provisioned and configured.

The federation farm uses the ADFS servers to provide claims-based authentication tokens, which can then be consumed by the Office 365 and other federated SaaS applications.

The ADFS infrastructure is installed into the Post Office production environment and hosted in the Azure UK South region. To support disaster recovery, all servers are replicated to the Azure UK West region. The service is comprised of two internal AD FS servers, two Web Application Proxy (WAP) and a single Azure Active Directory Connect server, synchronising user IDs and passwords.

Diagram below illustrate the design with all workloads located in Azure. Additionally, it illustrates the authentication processes for SaaS applications.

POL00337657

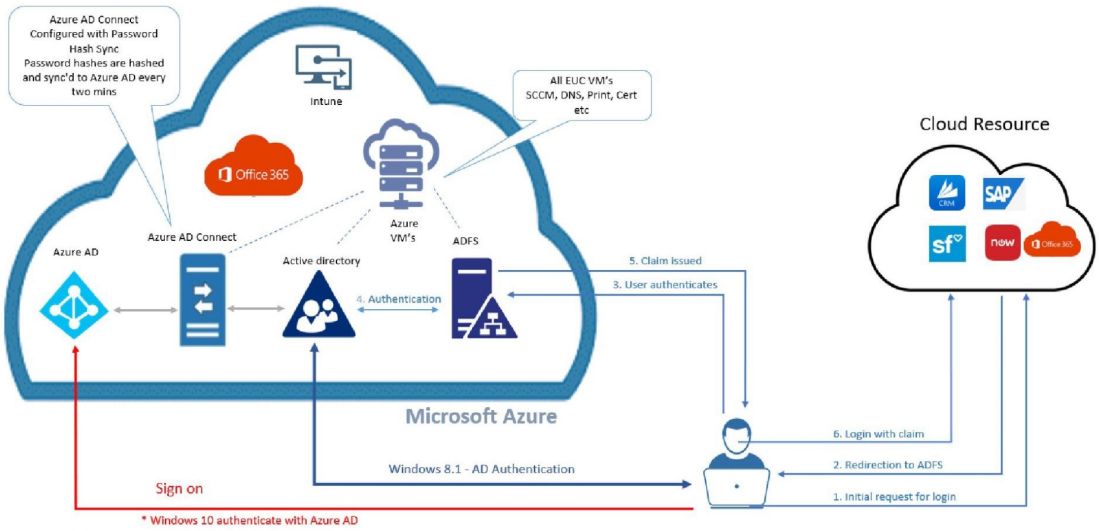


Figure 11: *Azure Workloads*

4.5.14 CViT Windows CE PDA's (Out of scope of EUC Contract)

CViT (Cash & Valuables in transit) Drivers currently use 350 Windows CE Devices running on Zebra MC65s PDA devices which are specialist devices that are supported by the supplier Barcode Warehouse. They are used to access the TransTrack mobile solution, which is used to track and control Cash pouches, delivered and accepted by its CViT vehicles.

The Zebra device hosts this as the sole application (boots to TransTrack). It has an in-built optical barcode scanner used to scan the cash pouches when loading vans / delivering to Postmasters. There is also a separate Bluetooth printer that is still used for interim receipt production.

Connectivity to the back office TransTrack application is achieved via docking stations which both charge and provide ethernet connectivity to the Post Office WAN. To pair a device to a router and retrieve (and submit) data the operator must enter the server IP and unique port (obtained from the back-office application) into the device. Once in the dock, the device will contact the server and synchronise data. The operator must wait for both ends to confirm synchronisation before removing the device from the dock.

The devices are managed using a legacy SOTi Mobile Device Management server. Currently the O/S (CE) is end of life, as is the Zebra MC65 device and the support partner are cannibalising old devices to keep the estate working.

4.5.15 CViT Android devices

A recent successful pilot of 20 Samsung Android devices at the Newton Abbot depot tested out a more modern infrastructure stack. This included the following technologies

- Microsoft Endpoint Manager for full MDM device management.
- Android devices (Samsung Tablets / Android Phones).

POL00337657

- Corporate Wi-Fi connectivity in the Depot.
- Over the wire route synchronisation.
- Zscaler mobile client to secure internet access.
- O365 Productivity stack (Teams, Yammer etc) for collaboration and knowledge sharing.
- The latest TransTrack Android client.

These devices now provide a small-scale production solution and therefore the support of these Android CViT devices is in-scope for the EUC contract

Post Office would like to evaluate the roll out to other depots in the future depending on the SCM strategic review work but with a fully managed device policy applied rather than a joint work / personal profile as in the pilot and will consider 5G when it has sufficient spread to cover the depot areas. Details of this potential future project are provided in Section 11.

4.5.16 Mimecast

Mimecast is an Email security tool used for Spam, Malware, Mail filtering and archiving. A plugin is installed in Outlook that would enable these security features on all devices.

Mimecast is also used for Data Protection searches for SAR / FOI and as such it is considered also as a compliance archive. This also includes the support for searches on the compliance archives.

4.5.17 Ironscales

Ironscales is a service that allows end uses to report phishing emails. Ironscales plugin is installed in Outlook that enables this security on all devices.

4.5.18 Managed Print (out of scope for EUC contract)

Delivery of the Managed Print service is the responsibility of the Managed Print supplier, however, the management and support of the required server infrastructure which delivers the FollowYou Print solution forms part of the scope of server hosting for the EUC supplier.

The Managed Print supplier remotely monitors print consumption and ink levels in MFDs. When toner levels become low on an MFD, the Managed Print supplier will ship toner to site, enabling a Post Office individual to replace the depleted toner with the fresh one. Paper for MFDs is provided by Post Office facilities.

The FollowYou Print solution is configured in both the Production (UK South Azure) & Pre-Production (UK West Azure) environments. The Pre-Production environment is configured as per the Production environment and is used for offline testing and patch testing prior to deploying to a live environment. Additionally, there is a ‘passive’ Disaster Recovery environment which is designed to be instigated in the UK West Azure Environment in the event of Data Centre failure in the UK South.

Although Managed Print is out of scope for the EUC contract, for the avoidance of doubt it should be noted that label and other non-standard branch printers which are listed as branch peripherals are in scope of support of the EUC contract.

4.5.19 Joiners, Movers and Leavers (JML)

POL00337657

Post Office have implemented an automated service for the Joiners, Movers and Leavers (JML) utilising Microsoft Identity Manager (2016 SP1). Microsoft Identity Manager (MIM) has been integrated heavily with active directory and is fully supported by the EUC Supplier. This includes patching the operating systems, antivirus, maintain the application, SQL database support and providing 3rd line level support.

The Platform is responsible for managing user lifecycle (joiner, movers and leavers) and Identity Data of internal (employees and contractors) users that exist in the HR system, SAP Success Factors. The platform is also used to manage access to several key Post Office systems.

The MIM Synchronisation Service is used to configure connectivity into the below connected identity data stores:

- SAP Success Factors.
- EUC Active Directory.
- Microsoft Exchange.
- File Servers.
- Teams.
- MIM Service.

The MIM Service and Portal is used for the configuration and management of the following:

- Provisioning / deprovisioning of users.
- Sets, workflows, policies and notifications.
- Group / Application management.
- User self-service (requests / approvals).

Microsoft identity Manager is hosted in Customer's Azure tenant, in a dedicated subscription called POL_Back_Office. This environment is currently connected using a dedicated Expressroute to the Customer's network. To further improve the design and optimise the network traffic, Post Office plans to migrate Microsoft Identity Manager to a dedicated Subscription in the main EUC Azure IaaS environment where shared technologies are hosted. From here, data is imported from SAP Success Factors and exported with Connectors to other data stores.

POL00337657

The diagram below shows a high-level logical architecture of the overall solution.

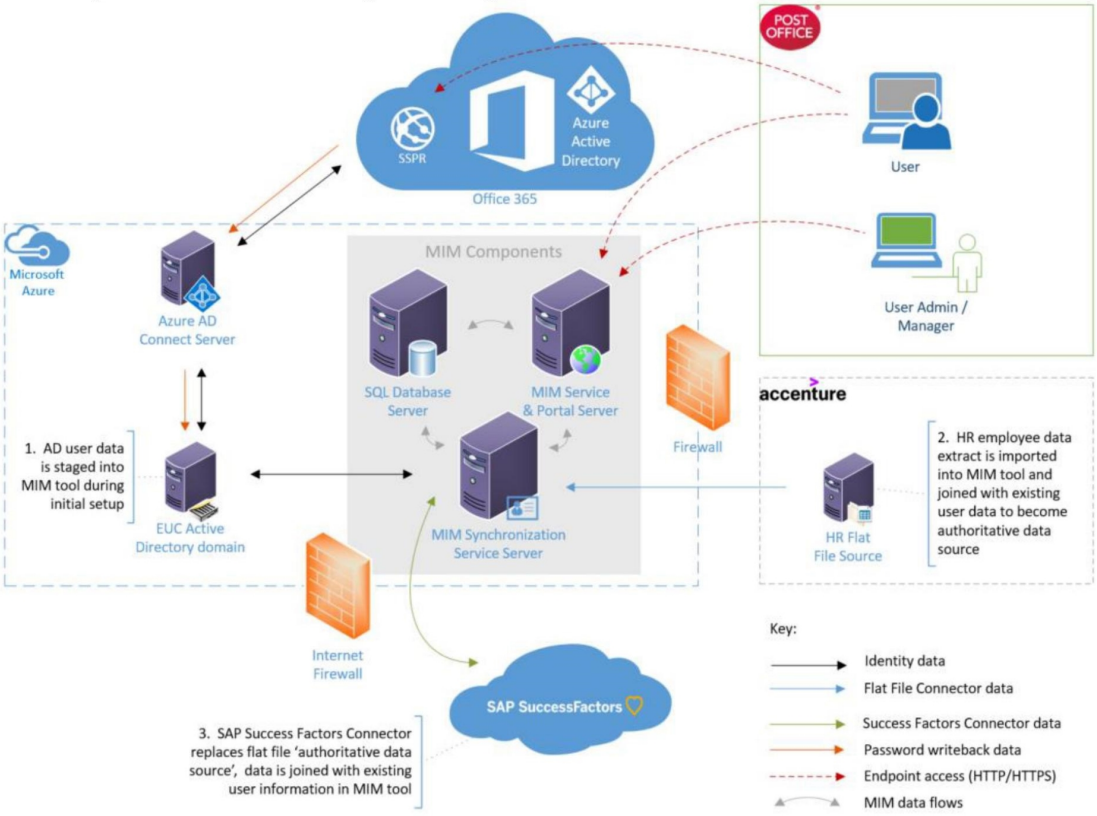


***Figure 12**: High-level architecture of the overall solution*

POL00337657

5. SERVICE OPERATING MODEL

5.1 Post Office Service Support Operating Model

Over the past 12-18 months, the Post Office has been transforming the way technology services are supported by our supplier partners. The Post Office has been moving from a largely outsourced Tower and SIAM model, to one where some of these services have been brought back into the Post Office, and others have been disaggregated and re-tendered as smaller more specific supply categories.

A key aspect of this transformation has been the insourcing of the service desk function and the service integrator responsibilities which are now delivered by the Post Office IT function.

Centered around our investment in the ServiceNow platform we have consolidated our 1st line service desk function from our Chesterfield Operations Centre. With a focus on supporting our Branch estate with user centric experiences modelled to deliver to their individual needs, this has been supported with investing in our IT Operations team to provide consistent ITIL operational practices.

As Post Office continues to mature SIAM capabilities, our intention is to follow recommendations from the Public Sector in onboarding new suppliers directly onto our instance of ServiceNow.

By adopting this model Post Office can consolidate services by:

- Having a consistent data source and providing visibility across services.
- Dynamically responding to events via workflow across the support and delivery supply chain.
- Lowering risk; lowering cost; improving speed, agility and service visibility.

Post Office IT delivery is largely aligned to the ITIL framework whereby work is carried out and coordinated under service processes (such as Request, Incident, Problem, Change). It is a blend between in-house and outsourced capabilities which deliver into a Post Office service integration layer.

EUC is an outsourced capability which depends on several internal capabilities such as the Service Desk, processes, and security operations.

5.1.1 Post Office IT Organisation

The Post Office IT organisation has 155 staff members and is organised into the following technology areas and organisational departments:

Technology Area	Organisational Department	# Staff
Service Desk (Service Integration)	Service Desk	24
End User Computing	Managed by current EUC Supplier	-
Networking	Managed by Verizon Business	-
Front Office (Branch Customer Facing Business Applications)	Branch & Digital Engineering (Front Office)	21
	Horizon & GLO IT (Front Office)	9
Cloud & Data Services	Cloud Centre of Excellence	15
	Data	
Security	Change & Technical Assurance	5
	InfoSec Compliance/Vendor Compliance	3
	Cyber Operations & Incident Management	10
	IT Controls	2
Service Management & Enterprise IT	Service Management	59

POL00337657

	Contract & Vendor Management	
	Solution Architecture	
Leadership	Senior Management	7

Table 10: *Post Office IT Organisation*

As well as Post Office having its own IT organisation capabilities, Post Office leverages third party suppliers to help complement their delivery of end to end services, and strong partnerships have been formed with multiple partners.

The following table provides the key IT function and who these areas are managed by:

Function	Managed by	Description
Service Desk	Post Office	The first point of contact for IT service for all users in the Post Office organisation (Branch and Colleague).
End-user Computing	Supplier scope of this tender process	Provide desktop and field services to Branch and Colleague.
Managed Print Service	Ricoh	Provide print services to Colleague.
Hosting	A mix of in-house teams and Suppliers	Physical server hosting, and Azure/ AWS cloud environments. (Note: EUC systems are delivered through Azure services and major Branch applications via AWS).
Networks	Verizon	Management of the Post Office networks including branch connectivity and network devices.
Front-Office	Fujitsu and Accenture	Provide Customer-facing applications which directly perform business functions. For Branch, Fujitsu support the single branch application, Horizon.
Back-Office	Accenture	Manage the back-end applications and enterprise database systems including POLSAP, HR SAP, CFS and FMI, Transtrack CWC, Traka32, Credence, Master Data Management (MDM) Business apps.
Cloud Team	Post Office	Management of the Azure and AWS cloud environments.
Branch Hub Support Team	Post Office	Management of the Branch Hub support and fulfilment delivery tools and processes.
ServiceNow Team	Post Office	Management and configuration of the ServiceNow ITSM toolset.
Information Security	Post Office	Responsible for defining and enforcing Post Office security policies.
Projects	Post Office	Management of the Post Office pipeline of projects.
Architecture	Post Office	Responsible for defining Post Office architecture standards, architectures that fall into their remit and governing supplier defined architecture.
Service Design & Transition	Post Office	Responsible for ensuring that new or changed services are defined, process integrated and handed over in line with the Post Office service requirements.
Process Teams	Post Office	Post Office has a number of process owners and teams e.g. Incident Management, Major Incident Management, Problem Management, Change Management and SACM. Suppliers feed into Post Office universal processes. Event Management is largely a supplier side activity.

Table 11: *Major Functions in the Post Office IT Organisation*

POL00337657

5.1.2 Service Model

The diagram below outlines the service model with Post Office acting as the service integrator.

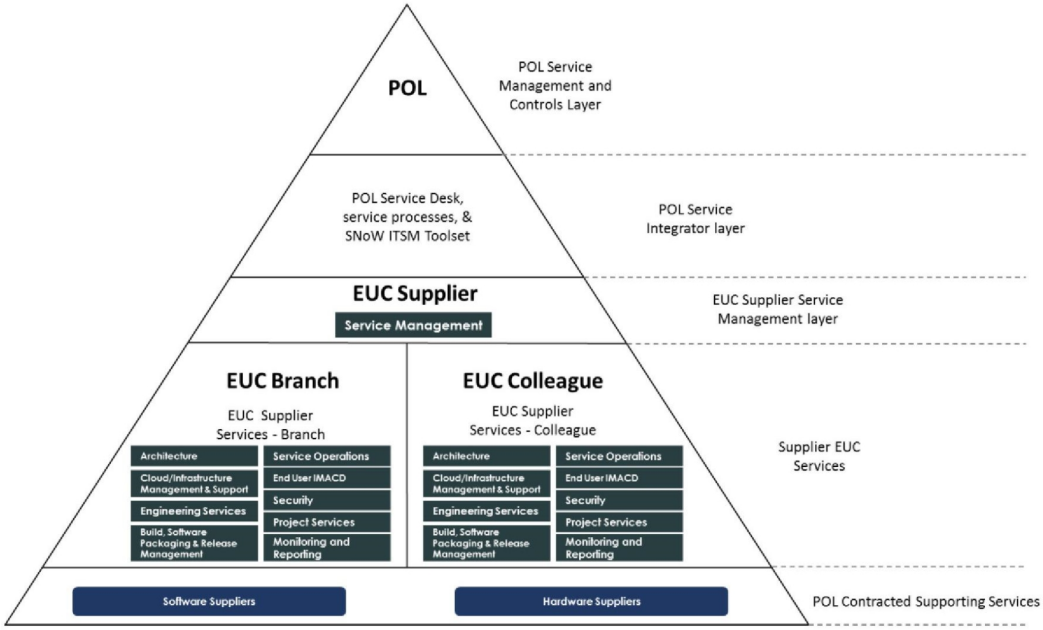
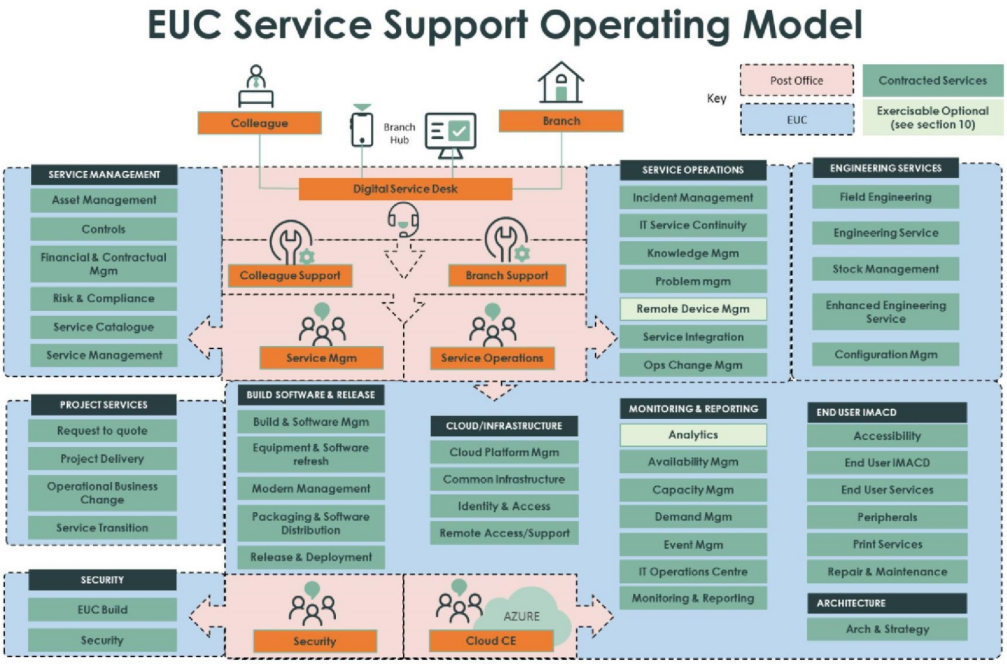


Figure 13: *Hierarchical view of the Supply Chain*

Post Office will always perform 1st line triage and attempt incident resolution or request fulfilment where possible. Should the 1st line teams not be able to achieve this, then they will functionally or technically escalate the incident or request to the appropriate next level in the hierarchy via the Post Office ServiceNow platform.
The EUC supplier will perform the role of 2nd & 3rd line as well as collaborating with Post Office 3rd line SMEs as and when appropriate.



POL00337657

Figure 14: *Support Model*

The EUC Supplier will deliver into a Post Office Service Integration layer which comprises of the Post Office Service Desk, universal processes, support model, and Service Management.

The EUC Supplier will provide services using an integrated mode of operations with Post Office, meaning that the EUC Supplier will work operationally as part-and-parcel of Post Office's IT and business operations. This includes using and supporting Post Office business processes and interfaces, and integrated process workflow pipelines e.g. request, incident, problem, change. To further enable this joint working the EUC Supplier will directly use Post Office's ITSM toolset which is ServiceNow.

The EUC Supplier's direct use Post Office's ServiceNow instance will avoid the need for using disparate ITSM tooling with e-bonding and will ensure a conformity of data and performance. With ServiceNow as a central data platform this will reduce the need for manual reporting though utilising performance analytics and reporting dashboards,

5.1.3 Split of Branch and Colleague

The EUC Services contract outsources the operational activities in terms of the Branch and Colleague EUC, while retaining the final say in terms of governance, design authority, service level management and the service/ process integration layer on which operations in the service are built.

The supplier should maintain a separation between service delivery to the Post Office Branch and Colleague business areas to ensure that services delivered to each of those business areas are delivered to meet the business requirements and operational practises of the business which are very different. Additionally, it is necessary to ensure that the impact of changes across these business areas is minimised.

By ensuring a clean separation between the two key business areas, the supplier will reduce complexity for Post Office and reduce the level of "plate-spinning" work which Post Office service management currently undertakes with regards to the current ways of working.

5.2 Incident Management

The following sections provide a description of how Post Office defines and managed the key area of Incident Management, detailing the separation of Incident Management from Major Incident Management, and providing the definition of Post Office's Incident Priority definitions.
The specific Incident Management requirements are further defined in the following section 6 Service Specification.

An Incident is defined as a P1 to P4 incident with regards to Post Office's internal incident definition detailed below.

The EUC Supplier will remediate IT incidents relating to the scope of the EUC service in order to minimise any related disruption to operations.

While the Post Office Service Desk will carry out an initial business impact prioritisation on incidents (based on urgency and impact), an incident record will be allocated to the EUC

POL00337657

Supplier to initiate the correct responses and resolve in-line with the corresponding Service Level Agreement.

The EUC Supplier incident priorities will be fully defined in the incident matrix which defines the criticality, impact, resolver groups and further important information and will be reflected in the CMDB for the corresponding Configuration Item.

The EUC Supplier will also perform Queue Management against all work item queues for which they are responsible, meaning that the EUC Supplier will proactively track and follow up on any outstanding work items and keep aged tickets to a minimum.

5.3 Major Incident Management

A Major Incident is defined as a P1 or P2 incident with regards to Post Office's internal incident definition, with P1 incidents receiving a greater degree of priority and visibility. Major Incidents are owned and managed by the Post Office Major Incident Management Team (MIM Team).

Upon a Major Incident, the Post Office Major Incident team requests that related suppliers and teams attend an incident bridge call for the duration of the Major Incident. The Post Office Major Incident Team produce or coordinate the Business Communications related to Major Incidents with technical and business impact support from the suppliers.

For all P1 & P2 incidents a problem record is automatically created, and a corresponding root cause analysis report will be undertaken by the resolving supplier in line with the Problem management requirement

The Post Office MIM Team operate during business hours, and additionally they are on call during all other hours. Similarly, the EUC Supplier is always expected to provide resources to attend Major Incidents.

The incident support model reflects the three key components of the EUC Service:

1. Infrastructure, Shared Services and Security.
2. Branch End user Services.
3. Colleague end user services.

5.4 Incident Priority Definitions

The Incidents are classified in order of priority 1-4 with a further set of service classifications and resolution times for Priority 3 Branch and Colleague end users.

Priority 1 & 2 Incidents are managed by the Major Incident Management process.
Priority 3 & 4 Incidents are managed by the Incident Management process.

The Incident Priority Definitions are provided below for each of the support model components.

5.4.1 Infrastructure, Shared Services and Security Incidents

Infrastructure and Security incidents covers the key platform, hardware, software and application used to deliver the EUC services and all elements of Security. The SLAs and response times reflect industry standards and best practice reflecting the urgency and criticality of restoring service and returning business operations with minimal impact and are covered by the priority definitions listed below:

POL00337657

- **P1** Major Incident
- **P2** Significant Incident
- **P3** Standard Incident
- **P4** Minor Incident

Incident Priority Level	Description	Examples	Resolution Target
P1 (Major Incident) Follows the Major Incident process for resolution	A material failure or outage that (i) affects the Customer IT infrastructure resulting in a loss of ability to trade, and/or deal with Customers, and/or settle or report to regulators, and/or satisfy any regulatory obligation, and/or (ii) results in potential or realised financial loss to Customer and/or damage to the reputation of Customer , and/or (iii) a significant impact to business operation (iv) Security: Data Loss, Malware, Denial of Service, Confirmed compromise	This is a Major Incident affecting entire sites, multiple departments or critical systems and applications running in a production environment or an agreed managed test environment. e.g.: • key application not Available with real business impact • directory services corruption resulting in an inability to login • Security breach • multiple counter functionality latency issues • multiple branches with reduced application functionality • collaboration and / or communication applications i.e. Teams failure	0 breaches of the 4 Hours resolution time

POL00337657

Incident Priority Level	Description	Examples	Resolution Target
P2 (Significant Incident) Follows the Major Incident process for resolution	A substantial but limited impact or potential failure or outage or partial outage that is (i) a degradation, failure or outage which has a serious internal impact that is likely to lead to delay or interruption to important, time critical working processes for a group and/or (ii) a failure or outage affecting multiple Users with no effective workaround. (iii) Security: Theoretical threat becomes active as a security P1 if not promptly addressed	Significant impact to business operations below the level of a P1 including test and non-production systems which have a significant impact on business operations. E.g.: • key batch processing failure • application not available with threat (as yet unrealised) of business impact • test system failure • security vulnerability • reduced branch application functionality • intermittent issues with a 'key application' or an issue with a key application that has an acceptable workaround • intermittent issues with email / communication platforms / directory services	0 breaches of the 8 Hours resolution time
P3 (Standard Incident) Follows the Incident process for resolution	An Incident that is not a Major Incident or a Significant Incident which requires a standard response and recovery. Security: Phishing email or active threat spreading infection	Noncritical application fault, single network connection failure, access constraints, solution available through workarounds.	98% within 12 Service Hours

POL00337657

Incident Priority Level	Description	Examples	Resolution Target
P4 (Minor Incident) Follows the Incident process for resolution	Any Incident that is not a Major Incident, a Critical Incident, or a Standard Incident. Security: Malware, phishing, miss configuration that could affects security	For example, a non-impacting threshold alert or non-urgent call. Non-critical issue to a test environment	98% within 24 Service Hours

Table 12: *Infrastructure & Security Incident Priority Definitions*

5.4.2 Branch P3 Incidents

Branch Incidents are for Incidents which impact a single Branch site. An incident impacting multiple (more than 1) Branches would be classified as an Infrastructure, Shared Services and Security P1 or P2 Incident and would follow the definition and response requirements described above.

All other Branch Incidents are defined as Priority 3 Incidents with the three levels of P3 categorisation and associated resolution requirements. These categories are defined below:

- **EUC-BR-ENG-01** (Major Branch Incident)
- **EUC-BR-ENG-02** (Standard Branch Incident)
- **EUC-BR-ENG-03** (Minor Branch Incident)

For the Branch estate the critical activity is ensuring that they can trade, and this is reflected in our requirements and Service Levels.

The Branch estate is made up of many different branch configurations, with a large proportion of the Branch Network being single trading counter branches, where even a peripheral failure can result in a branch not being able to serve the Customers that depend on the Post Office.

The Post Office openly acknowledging the challenges of delivering services to very remote locations, and from that standpoint uses an approach of grouping branches based on geographic location and assigning an SLA response time for physical visits.

The table below identifies the branch types, criteria and Service Levels for a Major Branch Incident, based on the EUC segmentation of Branches into City & Town; Urban; Rural; and Remote.

A number of Exception locations are also defined, including Non-Customer Facing; Island Exceptions; and Outreach locations.

POL00337657

	Name	Description	Criteria 3NrstDist	Service Level	Notes
1	City & Town	A Branch situated within a large settlement	<2	4 hours	c 4500 Branch's
2	Urban	A Branch situated close to a large settlement	2 - 6	5 hours	c 4700 Branch's
3	Rural	A Branch situated within a settlement in open country	6 – 10	6 hours	c 420 Branch's
4	Remote	A Branch situated within a settlement in open country with a large separation from a neighbouring branch; a Island with good transport links; a island with large population	>10 or Blank	12 hours	c 170 Branch's
Exceptions List – Branch's by local agreement					
5	Non customer facing	A Branch that does not trade with the general public	N/A	N/A	c 19 Branch's
7	Island Exceptions	A Branch situated on a remote island with restricted access	Blank	N/A	c 109 Branch's
8	Outreach	A Branch that is operated out of local buildings, such as village halls or community centres, and a fleet of mobile post office vans maintained by a central Post Office	N/A	N/A	c 1600 Branch's

Figure 15: *Branch Segmentation types and Exceptions*

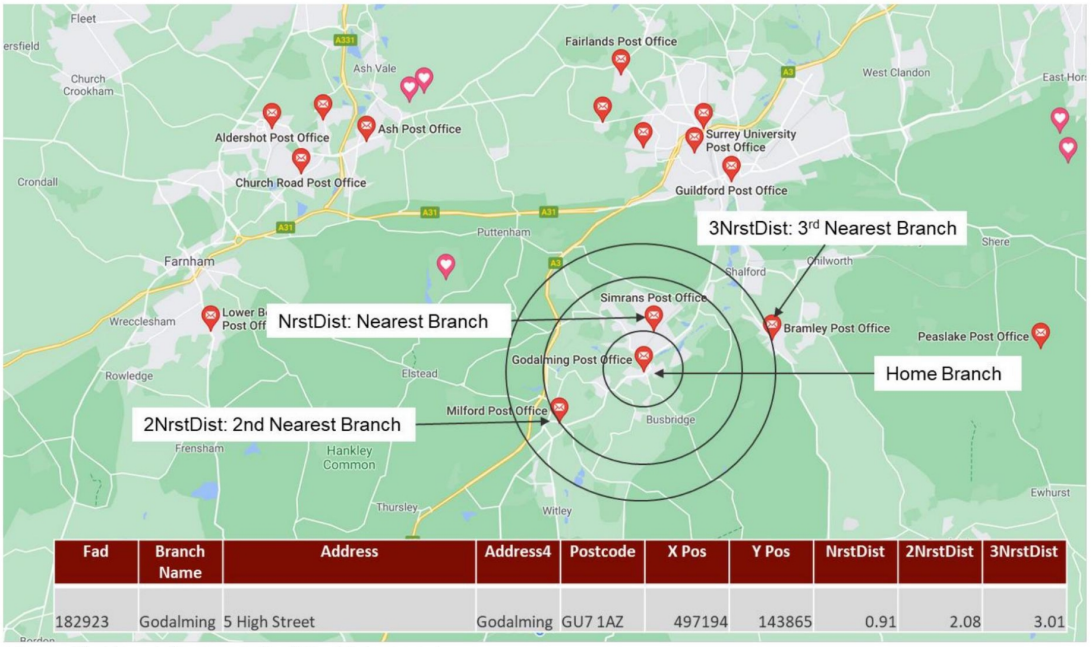
Each Post Office Branch has been geo-tagged, and the 3 nearest branches have been identified and a distance recorded for each of these branches:

- NrstDist = nearest distance to the next branch
- 2NrstDist = 2nd nearest distance to a branch
- 3NrstDist = 3rd nearest distance to a branch

The more remote a branch is, the larger the NrstDist number is (recorded as miles). By using the 3NrstDist number it provides an accurate indicator on how remote or how central a branch is to others.

Using the 3NrstDist metric, branches are allocated to EUC segmentation locations (City & Town, Urban, Rural and Remote) with a corresponding field engineering response time.

The picture below is an example of a branch and the 3 nearest branches. As the 3NrstDist has a measure of 3.01 this results in the branch being classified as Urban and will receive a 5 hours field engineering response time.



Fad	Branch Name	Address	Address4	Postcode	X Pos	Y Pos	NrstDist	2NrstDist	3NrstDist
182923	Godalming	5 High Street	Godalming	GU7 1AZ	497194	143865	0.91	2.08	3.01

Figure 16: *Branch Segmentation3NrstDist example.*

POL00337657

The EUC supplier will need to work with Post Office departments (Branch estate, IT Service Management, etc) to create innovative support solutions to better service the Branch estate in order to meet the Service Levels and requirements. For example, a managed stock of replacement parts and spares in remote locations utilising the Post Office estate as depos and utilising postal services to aid Branch break-fix, so Branches can mail back and receive replacement parts.

Remote Locations and Exceptions: The EUC Supplier will need to support the Branch estate's full geographical locations, which covers very remote locations from the Eastern Isles to Shetland that provide critical services to their communities. Supporting these types of Branches takes diverse solutions to ensure they receive, wherever possible, the same level of service as the rest of the Network. Transport links to these locations are often infrequent, for example ferries twice per week or need special access arrangements.

Again, working with the Post Office the supplier will need to provide alternative solutions via utilising Postal Services, remote support and direct access to spares to enable the branches to resolve issues as quickly as possible and commence trading.

Outreach Branches: There are also a number of outreach branches, meaning mobile branches operated in public locations on a temporary basis, or which travel to the homes of Customers (Post Office van services). It is assumed that outreach branches will drop off any equipment relating to engineer visits at their parent branch locations, and SLAs in respect of visits to outreach branches will be dependent on this. There is sometimes the need for an engineer to support an outreach location and this will be arranged in conjunction with the Postmaster, Post Office support teams and the supplier (with reference to the SLA exceptions above).

Please refer to **Appendix A: Ref Doc-007-Branch and Colleague Locations** for a full list of Branch allocations to the EUC Segments: City & Town; Urban; Rural; and Remote (and identification of the exception locations: Non-Customer Facing; Island Exceptions; and Outreach).

POL00337657

Branch P3 Categories	Description	Examples	Resolution time
EUC-BR-ENG-01 (Major Branch Incident) Follows the Incident process for resolution	A failure or outage that (i) results in a complete failure of an individual Branch to trade, and/or deal with Customers, and/or (ii) a significant impact to business operation for a multi-counter branch (iii) actual financial impact to the Postmaster or Reconciliation or Cash Management impact to the Postmaster	This is an Incident affecting a single branch that cannot trade. Multiple branches with reduced functionality or application running slowly • single counter branch unable to trade • multiple counter branch with 75% reduced availably • Inability to provide essential Branch services such as Gas / Water / Electricity Bill Pay / Pre-Pay OR ability to access/Deposit Cash	95% within: 4 Service Hours for City & Town Branches 5 Service Hours for Urban Branches 6 Service Hours for Rural Branches 12 Service Hours for Remote Branches
EUC-BR-ENG-02 (Standard Branch Incident) Follows the Incident process for resolution	Branch IT fault with reduced counter functionality and/or solution available through workarounds for single counter branch. Branches with up to 75% counter failure.	Single Branch IT fault with a workaround. Multi counter branch counter Branch with two counter failure. Reduced counter functionality, with workarounds.	95% within: 24 Hours for City and Town, Urban and Rural branches 36 Hours for: Remote branches
EUC-BR-ENG-03 (Minor Branch Incident) Follows the Incident process for resolution	Branch Requests or non-urgent call or Postal service.	Non critical peripheral fault, replacement cable or postal service request	95% within: 48 Hours for: City and Town, Urban and Rural branches 72 Hours for Remote branches

Table 13: *Branch P3 Incident Priority Sub-Categorisation*

5.4.3 Colleague and Supply Chain P3 Incidents

POL00337657

The Colleague Incident categories are defined to reflect the impact within support roles for our Colleague and corporate environments and the delivery of key business applications in the running of the Post Office.

Similar to Branch Incidents, Colleague and Supply Chain Incidents which impact multiple Colleagues/Colleague Locations due to a material or significant IT failure would be classified as an Infrastructure, Shared Services and Security P1 or P2 Incident and would follow the Major Incident Management process and response requirements described above.

All other Colleague and Supply Chain Incidents are defined as Priority 3 Incidents with the three levels of P3 categorisation and associated resolution requirements. These categories are defined below:

- **EUC-CO-ENG-01** (VIP Colleague Incident)
- **EUC-CO-ENG-02** (Significant Colleague Incident)
- **EUC-CO-ENG-03** (Standard Colleague Incident)

Colleague P3 Categories	Description	Examples	Resolution time
EUC-CO-ENG-01 (Colleague VIP Incident) Follows the Incident process for resolution	A failure or outage of an end user device, software, application or EUC end user services that is linked to a VIP.	This is a high priority incident that is affecting a VIP user from conducting their business activities either end user hardware, software or key applications e.g. • Laptop Failure • Office365 availability • Security breach • Network connectivity	98% within 4 Service Hours
EUC-CO-ENG-02 (Colleague Business Critical User Incident) Follows the Incident process for resolution	A failure or outage of an end user device, software, application or EUC end user services that is linked to a business-critical user.	This is a priority incident that is affecting a business-critical user from conducting their business activities either end user hardware, software or key applications e.g. • Laptop/Desktop Failure • Office365 availability • Security breach • Network connectivity	98% within 8 Service Hours

POL00337657

Colleague P3 Categories	Description	Examples	Resolution time
EUC-CO-ENG-03 (Colleague Standard Incident) Follows the Incident process for resolution	A failure or outage of an end user device, software, application or EUC end user services that is linked to a non-critical user.	Noncritical application, connectivity or hardware fault for a single user.	98% within 12 Service Hours

Table 14: *Colleague P3 Colleague Incident Priority Definitions*

POL00337657

6. SERVICE SPECIFICATION

This section describes the requirements for the ongoing service required by the Post Office. The EUC Supplier is required to provide a solution that supports all of the Services specified in this section for the Technology Framework described in Section 4 above, within the framework of the Operating Model defined in Section 5 above. All Services unless otherwise specifically stated, are included in the Service Charges. The Supplier shall be responsive, adapting to the current and future requirements of Post Office and in doing so will be committed to an approach of providing continuous service improvement by proactively anticipating needs and adjusting services accordingly.

The high-level service model is comprised of the following service categories which are described below and accompanied by the detailed service requirements:



Figure 17: *EUC Managed Service – Service Capabilities (Requirements)*

6.1 Service Operating hours

POL00337657

Service Operating Hours	
Architecture,	8am – 6pm Monday – Friday excluding Public bank holidays
Service Management,	8am – 6pm Monday – Friday excluding Public bank holidays
Project Services,	8am – 6pm Monday – Friday excluding Public bank holidays
Build, Software Packaging	8am – 6pm Monday – Friday excluding Public bank holidays
End user IMACD	8am – 6pm Monday – Friday excluding Public bank holidays
Cloud/infrastructure Management & Support	8am – 6pm Monday – Friday excluding Public bank holidays
Engineering Services including Field Engineering Service, Service Operations,	8am - 8pm Monday – Friday excluding Public bank holidays 08:00 to 16:00 Saturday – Sunday
Monitoring and Reporting,	24hr a day all year
Major Incident Management (priority 1 and 2 incidents)	24hr a day all year
Release Management	24hr a day all year
Security	24hr a day all year

Table 15: *Service Operating hours*

6.2 Architecture

This service area provides Architecture capabilities to Post Office to support the design and assurance of changes to the Post Office EUC environment. The Supplier shall provide their processes, tools, methodologies and experiences in all aspects of business and technology architectural change in the Post Office IT services within the scope of EUC Services.

6.2.1 Architecture and Strategy:

Architecture and Strategy defines the structure of Post Office Systems or IT services, including the relationships of components to each other and to the environment they are in. Architecture also includes the Post Office Standards and Guidelines which guide the design and evolution of the solutions.

Req. ID	Requirement Description
EUC-AS-01	The Supplier shall, at all times adhere to the Customer's Architecture and Security Standards in the delivery of their Services.
EUC-AS-02	The Supplier shall, contribute to the Customer's Enterprise Architecture Standards relevant to its services as required.
EUC-AS-03	The Supplier shall, be compliant with the Customer's Enterprise Architecture Standards including verification that all changes comply. If requested, the Supplier shall produce a summary of compliance/non-compliance architecture standards reports for the Customer.
EUC-AS-04	The Supplier shall, implement, track and report on agreed remediation actions in respect of any non-compliance with the Customer's Enterprise Architecture Standards.

POL00337657

EUC-AS-05	The Supplier shall, provide an EUC architecture reference model showing the EUC capabilities provided as part of the service and technology platforms / architecture patterns used to deliver the services.
EUC-AS-06	The Supplier shall, assist the Customer in developing and updating roadmaps, IT systems, processes, technical architecture and standards. The Customer's roadmaps will be developed, on a quarterly basis, and stored in the Customer's architecture repository. This shall include a rolling three (3) year projection of anticipated changes (subject to the Customer's business and planning requirements).
EUC-AS-07	The Supplier shall, support the Customer by participating in a monthly architecture review forum regarding: (a) review of the current infrastructure; (b) risk, issues and changes where they are aware of such; (c) development plans; and (d) performance and capacity.
EUC-AS-08	The Supplier shall, support the Customer by participating in a quarterly architecture review forum regarding: (a) equipment and software architecture and standards; (b) industry and technology trends; (c) regulatory issues/changes where they are aware of such; (d) data and lessons learned from the Operating Environment; (e) trend analysis from data to predict future demand; (f) good practice from their other accounts and centres of excellence; and (g) any element of the infrastructure or architecture which is forecast to go end of life within the following 12 months and includes configuration which may be depreciated due to releases.
EUC-AS-09	The Supplier shall, provide an architectural engineering function to include, but not limited to: - (a) producing technical designs and support requirements to meet the Customer's architecture and security standards in the management of the Infrastructure; (b) provide As-Is and transitional architecture states to assist with project delivery (to be included in any new Solution Design documents); (c) ensuring all solution designs have traceability to functional and non-functional requirements; (d) presenting solution designs to Customer's Architecture Governance Committees to get approval and make amendments to designs based on feedback from Architecture Governance Committees and re-present as required; (e) translating Customer's architecture requirements into specific configuration and deployment templates; (f) developing and propose new or enhanced Infrastructure plans and designs on an on-going basis; (g) producing required documentation and updates in accordance with the Customer's ITIL Service Management Processes; and (h) engineer the Infrastructure to provide optimisation and increased efficiencies including cost controls.
EUC-AS-10	The Supplier shall, where developing or upgrading technical solutions, make considerations for enabling action to be taken at first line support.

POL00337657

EUC-AS-11	The Supplier shall, as agreed with the Customer, provide and maintain in scope middleware components available on the End User Device.
EUC-AS-12	The Supplier shall, in collaboration with Customer's Technical Architects support the following: (a) review platform selection decisions and provide technical support and configuration advice; (b) review Customer business cases and suggest alternatives as needed. (c) participate in proof-of-concept projects, including suggesting industry best practices. (d) contribute to or develop requirements and statements of works for new technologies and architectures with a view to improving Customer experience of the services provided; (e) provide analysis and input to support the ongoing design and configuration standards for architectural purposes; and (f) update and provide documentation as architectural designs and decisions are approved.
EUC-AS-13	The Supplier shall, share with the Customer their internal technology and innovation disciplines, to bring continual innovation, enhancements and industry best practice to the Customer's End User Computing solution.
EUC-AS-14	The Supplier shall, maintain within the Customer's architecture repository, Technical Design documents, ensuring they are updated for material or significant changes.
EUC-AS-15	The Supplier shall, maintain the Customer's low-level Designs ensuring they are updated for material or significant changes and be visible to the Customer in real-time for searching and querying.
EUC-AS-16	The Supplier shall, provide a dedicated Customer Operational Architect (COA) resource on a full-time basis who will work as an integrated member of the Customer and the Supplier's EUC infrastructure engineering function, and with other suppliers or subject matter experts as required.
EUC-AS-17	The Supplier shall, attend Customer Architecture Review Boards and provide input in line with Customer's architecture governance framework.
EUC-AS-18	The Supplier shall, as requested by the Customer, perform architecture impact assessments for evergreen Platform as Service (PaaS) or Software as a Service (SaaS) services to ensure any changes are identified and impact is understood.
EUC-AS-19	The Supplier shall, be responsible for paying all costs associated with: (a) licenses for their software; and (b) packaging all of the Customer's 'official' software, when requested by the Customer.
EUC-AS-20	The Supplier shall, continually review documentation to ensure: (a) DR and ITSCM commitments are upheld for any changes; (b) any architecture changes are regression tested against the existing environment to ensure no breaking changes are introduced.
EUC-AS-21	The Supplier shall, provide representation and support for technical change reviews relating, but not limited to: (a) Technical CAB, (b) CAB; (c) DR; and (d) Major incidents etc.

POL00337657

EUC-AS-22	The Supplier shall, deliver all services, where applicable, to PCI legislation and compliance activities associated with, but not limited to infrastructure, engineering, operations and processes.

6.3 Cloud / Infrastructure Management & Support

Setup, configure, run, monitor, and optimise the components of Post Office cloud infrastructure related to EUC. Manage Post Office's Back-end services, which includes resource groups and other related tasks, within the cloud environment.

6.3.1 Common Infrastructure Services

The provision on IT systems and software for the delivery of EUC Services to Post Office Colleague and the Branch estates.

Req ID	Requirement Description
EUC-CIS-01	The Supplier shall, provide, manage and work with Customer and the relevant Suppliers to implement the EUC Infrastructure solution and in accordance with the Customer's Security Standards.
EUC-CIS-02	The Supplier shall, work co-operatively with the Customer and Third Party Vendors in optimising and implementation EUC Infrastructure services.
EUC-CIS-03	The Supplier shall, maintain synchronisation of the EUC servers and Access Devices within agreed time sources and the Master Time Reference provided by the Customer or nominated agent.
EUC-CIS-04	The Supplier shall, provide and maintain Directory Services (Pre-production and Production). The pre-production environment must reflect the production environment.
EUC-CIS-05	The Supplier shall, enable other Third-Party Vendors to utilise the Directory Services, in order to commission additional services for which there may be a reliance on components of the Directory Services.
EUC-CIS-06	The Supplier shall, support and maintain the infrastructure, the integrity of replication and quality of data used for directory replication within Domain Controllers.
EUC-CIS-07	The Supplier shall, ensure Authentication Services comply with the Security Requirements, Security Policy and processes.
EUC-CIS-08	The Supplier shall, support and deliver 2FA / MFA as required by the Customer.
EUC-CIS-09	The Supplier shall, maintain and support the Authentication Technology Service for all Users and Access Devices.
EUC-CIS-10	The Supplier shall, provide an Azure Active Directory (AAD) and Active Directory (AD) integration capability that enables single sign on and Authentication Services for Users where applications are configured to use Active Directory as the main authentication method.
EUC-CIS-11	The Supplier shall, extend the single sign on service (where technically possible through the AD and AAD) to add such new applications as may be specified by the Customer.

POL00337657

EUC-CIS-12	The Supplier shall, ensure that the Authentication Services enable Users to logon to an appropriate connected Access Device so that the User may securely access applications, print services and data for which they are authorized.
EUC-CIS-13	The Supplier shall, maintain Remote Access Service (RAS) configuration information provided by the Customer or nominated Third party in the deployed VPN clients.
EUC-CIS-14	The supplier shall, manage and administer directory services, included but not limited to: (a) configuration management; (b) group policy management; (c) topology and replication management; (d) schema management; (e) user and group account administration; (f) reporting; (g) monitoring connectivity; (h) net logon and trust relationships; and (i) replication.
EUC-CIS-15	The Supplier shall, support and enable Internet access for all in scope devices through automation and policies subject to the security constraints.
EUC-CIS-16	The Supplier shall, process Service Requests relating to the Directory platform, in accordance with the Customer policies and subject to the security constraints.
EUC-CIS-17	The Supplier shall, provide Operational Support and maintenance of the Customer's Directory Services.
EUC-CIS-18	The Supplier shall, manage administration and system accounts in accordance with the Customer account management Policy. Where these policies do not exist, the Supplier shall ensure Industry Best Practice in agreement with the Customer.
EUC-CIS-19	The Supplier shall, provide Operational Support of the in-scope Public Key Infrastructure (PKI) platform certificate services which are hosted in the Cloud.
EUC-CIS-20	The Supplier shall, create, authorise, issue, renew and revocation of certificates in accordance with the Customer's policies. Where these policies do not exist assist in the development of policies and standards.
EUC-CIS-21	The Supplier shall, respond to service requests related to PKI certificates associated with the Services.
EUC-CIS-22	The Supplier shall, monitor their sub CA PKI database of issued certificates to identify if any certificates are nearing expiry and shall report these, with recommendations to the Customer at agreed intervals.
EUC-CIS-23	The supplier shall, manage, maintain and administer the Customer's Domain Name System (DNS) services. This includes creation, management and administration of DNS records and zones for computers, services, or other resources connected to the Internet or a private network.

POL00337657

EUC-CIS-24	The Supplier will perform Azure Virtual Machine Back up Service in line with the following schedule: (a) Retention of Daily Backup Point Retention Range For: 14 Days (b) Retention of Weekly Backup Point Retention Range On: Sunday For: 4 Weeks (c) Retention of Monthly Backup Point Retention Range On: Last Day: Sunday For: 6 Months (d) Retention of Yearly Backup Point Retention Range In: January On: Last Day: Sunday For: 1 Year

6.3.2 Identity and Access Management

The process of defining and managing the roles and access privileges of End Users and the circumstances in which End Users are granted or denied those privileges.

Req ID	Requirement Description
EUC-IAM-01	The Supplier shall, ensure that the Identity and Access Management Service supports the Customer's Access Management Standard including the ability to audit and attest.
EUC-IAM-02	The Supplier shall, make the Identity and Access Management Service available to the Customer's Security Information and Event Management (SIEM) platform in near real time for analysis, incident management and assurance, and make available to other Suppliers to support the Asset Management Standard – Access Control Standard.
EUC-IAM-03	The Supplier shall, implement and enforce the Customer's Password Management Policy covered under Access control standard for the Identity and Access Management Service, unless otherwise agreed with the Customer.
EUC-IAM-04	The Supplier shall, in agreement with the Customer, create the Identity and Access Management Service processes and Procedures in accordance with the Customer's Access Management & Control Standards.
EUC-IAM-05	The Supplier shall, enable the capability for Customer Services to query the Identity and Access Management Service Master Directory.
EUC-IAM-06	The Supplier shall, manage, maintain and support Connectors to enable the provisioning and synchronisation of identity and attribute data.
EUC-IAM-07	The Supplier shall, work collaboratively with Third Party Suppliers to agree a specification for any new Connector, including but not limited to: (a) Third Party attributes to be synchronised to the Customer's Master Directory; (b) Customer's attributes to be synchronised from the Master Directory to Third Party Suppliers; and; (c) frequency of synchronisation.
EUC-IAM-08	The Supplier shall, in agreement with the Customer, ensure the Identity and Access Management Service synchronises with identity and attribute data between Identity and Access Management Service and the systems provided by the Third-Party Suppliers and the Customer.
EUC-IAM-09	The Supplier shall, in agreement with the Customer, work with Third Party Supplies to grant the required access to the Customer's Services.

POL00337657

EUC-IAM-10	The Supplier shall, manage, maintain and support a Federated Identity and Access Management capability for the Customer Services and Third-Party Suppliers.
EUC-IAM-11	The Supplier shall, provide, maintain and support a self-service password management function in accordance with the Customer's Access Control Standard. This update is to be synchronised to all applicable target Services.
EUC-IAM-12	The Supplier shall, provide, maintain and support a secure self-service facility to allow End Users or Customer representatives to amend agreed personal attribute information held within the Identity and Access Management Service.
EUC-IAM-13	The Supplier shall, work and collaborate with the Customer to ensure that the Supplier's self-service facility is delivered through the Customer's Azure self-service portal.
EUC-IAM-14	The Supplier shall, configure and support the Identity and Access Management Service such that any change synchronises all data to target Services within one (1) hour of the change being committed on the originating system.
EUC-IAM-15	The Supplier shall, be responsible for the management and support of the Customer's Shared Services platform hosted in the Customer's Cloud tenant.
EUC-IAM-16	The Supplier shall, be responsible for the management of shared services technologies including but not limited to, directory services, dynamic naming system, system configuration utilities, certificate and PKI services, end point management.
EUC-IAM-17	The Supplier shall, be required to manage the Customer's EUC Cloud landing zone, subscriptions and services, in adherence with Customer's cloud policies.
EUC-IAM-18	The Supplier shall, ensure access to the meta data in the form of log ingestion to SIEM for PIM/PAM and SSO and support Security Incident management directly with the Customer's Security Operations Centre (SOC).
EUC-IAM-19	The Supplier shall, provide the Customer with the reports necessary to conduct assurance reviews, in relation to general access and privileged access control.

6.3.3 Remote Access and Support

The provision of IT infrastructure for end users who are remotely working away from corporate networks in order to access Post Office systems.

Req ID	Requirement Description
EUC-RAS-01	The Supplier shall, in conjunction with other Third-Party Suppliers, ensure that End Users have secure remote access to the Customer's internal network and services.
EUC-RAS-02	The Supplier shall, provide software deployment and patch distribution for remote End Users in accordance with information security policies and procedures.

POL00337657

EUC-RAS-03	The Supplier shall, provide software updates as per policy in emergency situations (for example, malware, security threats) to remote End Users. The distribution of the software updates to End Users will be automatically executed upon connection.
EUC-RAS-04	The Supplier shall, provide solutions according to policy, to protect equipment that is directly connected to the internet by use of end point security solutions that meet or exceed Industry Standards.
EUC-RAS-05	The Supplier shall, ensure that all remote End Users can access a centrally provided file and print service in all sites.
EUC-RAS-06	The Supplier shall, provide integration (in the form of log ingestion into the Customer's SIEM solution) for, but not limited to Access Management meta data.
EUC-RAS-07	The Supplier shall, provide support for Security Incident Management directly with the Customer's Security Operations Centre (SOC).

6.3.4 Cloud Platform Management

Management and supporting of Post Office's EUC Cloud Infrastructure as a Service providing computing infrastructure, provisioned and managed over the Internet.

Req ID	Requirement Description
EUC-CPM-01	The Supplier shall, support and maintain appropriately resilient and available cloud hosted solutions in accordance with defined business and/or technical requirements (BC/DR/HA).
EUC-CPM-02	The Supplier shall, provide appropriate mechanisms and processes for: (a) the purpose of detection and prevention of unauthorised cloud hosted data loss; (b) detection and prevention of data loss (DLP) (c) privileged access management; and (d) account management.
EUC-CPM-03	The Supplier shall, provide appropriate mechanisms and measures to protect cloud hosted systems from threats, which includes but is not limited to Anti-Virus and Anti-Malware.
EUC-CPM-04	The Supplier shall, provide appropriate mechanisms and processes to manage cloud data ingress/egress, which includes but is not limited to Firewall management and Route management.
EUC-CPM-05	The Supplier shall, provide appropriate integration with Identity Management Services, to authenticate and grant permission to End Users, applications, Services and other resources (IAM).
EUC-CPM-06	The Supplier shall, provide and be responsible for appropriate measures to support Role Based Access restrictions (RBAC).
EUC-CPM-07	The Supplier shall, provide appropriate mechanisms and measures to identify, assess and report on system and resource threats.
EUC-CPM-08	The Supplier shall, provide mechanisms and processes to maintain the security of cloud-based applications, systems and services, which includes but is not limited to: (a) patching; (b) software/system upgrades; and (c) vulnerability management scanning logs.

POL00337657

EUC-CPM-09	The Supplier shall, in accordance with defined polices and best practices, provide appropriate mechanisms and measures to identify, assess and report on system wide compliance, which includes but is not limited to applications and platform configuration.
EUC-CPM-10	The Supplier shall, provide appropriate mechanisms to manage system, application and service credentials, which includes but is not limited to Managed Secrets and the management and monitoring of EUC SubCA Certificates services.
EUC-CPM-11	The Supplier shall, provide appropriate mechanisms and processes to gather and distribute security log and alert data for the purpose of monitoring and analysing the Customer security posture (SoC-integration).
EUC-CPM-12	The Supplier shall, provide appropriate mechanisms and processes to gather, collate and present cloud resources and services for cost/charge information.
EUC-CPM-13	The Supplier shall, provide appropriate mechanisms and measures to analyse, report and act upon system/resource usage, which includes but is not limited to resource rightsizing and instance reservation.
EUC-CPM-14	The Supplier shall, provide appropriate mechanisms and processes to gather and distribute log data for the purpose of operational monitoring and analysis (Log Management).
EUC-CPM-15	The Supplier shall, provide appropriate mechanisms and processes to gather, report and act upon application, system and service level events (Event Management).
EUC-CPM-16	The Supplier shall, provide appropriate mechanisms to dynamically report on cloud-based application and resource state, which includes but is not limited to: (a) resource/service dashboards; (b) metric analysis; and (c) status reports.
EUC-CPM-17	The Supplier shall, provide mechanisms and processes to update cloud-based applications, services and systems through appropriate patching and/or software/system upgrades, which includes but is not limited to: (a) maintenance updates; and (b) functionality enhancements.
EUC-CPM-18	The Supplier shall, organise and facilitate a monthly management meeting to report on in-scope cloud hosted resources, which includes but is not limited to current usage and performance to represent target solution forecast metrics.
EUC-CPM-19	The Supplier shall, provide appropriate mechanisms and processes to ensure cloud hosted applications, services and systems are backed up in accordance with solution requirements, which includes but is not limited to: (a) IaaS platform VMs and installed applications (SQL); and (b) periodic system and data restores being tested in accordance with the solution and Customer's requirements.
EUC-CPM-20	The Supplier shall, in accordance with defined security and retention polices, provide mechanisms and measures to ensure all cloud hosted data is stored securely and managed appropriately.

POL00337657

EUC-CPM-21	The Supplier shall, provide appropriate mechanisms to ensure cloud hosted applications, services and systems can be recovered in accordance with defined business and/or technical solution requirements (RTO/RPO/RTA).
EUC-CPM-22	The Supplier shall, provide mechanisms and processes to ensure cloud hosted resources can be easily identified (Enforce tagging/labelling).
EUC-CPM-23	The Supplier shall, support the provisioning of cloud services and infrastructure through code (IaC) and include continuous integration and delivery (CI/CD).
EUC-CPM-24	The Supplier shall, provide, support and be responsible for all associated costs for the appropriate integration with the Customer Service Management Platform (ITSM).
EUC-CPM-25	The Supplier shall, ensure integrations with ITSM and SIEM platforms which includes, but not limited to: (a) DLP; (b) Anti-Virus; (c) Anti Malware; (d) Firewall Management; (e) IAM; (f) RBAC; and (g) Vulnerability Management.

6.4 Engineering Services

This service includes:

- Engineering Support Services – Second line support function for the restoration and delivery of services in the Branch and colleagues.
- Enhanced Engineering Services - A Colleague VIP Engineer service (2nd Line) which includes providing support engineers for both office-based and remote workers; and
- Field Engineering Service – For the Branch estate as an extension of our branch support/management team capable of supporting all Postmaster needs.

6.4.1 Engineer Support Services

Second line support function for the restoration and delivery of services in the Branch and colleagues.

Req ID	Requirement Description
EUC-ES-01	The Supplier shall, provide engineering support when requested by the Customer to assist with network connectivity and hardware at Customer sites to include, but not limited to:- (a) Router (Inc. WIFI and Cellular); (b) Switches; (c) Hubs; (d) Cabling.
EUC-ES-02	The Supplier shall, resolve Incidents associated with equipment and software failure or degradation of in-scope assets or services and infrastructure under the supplier provision and provide in line with Service Level agreements:

POL00337657

	(a) break/fix support; (b) remote fix; (c) configuration support/fix (d) access support/fix (e) advice; and (f) assistance to End Users.
EUC-ES-03	The Supplier shall, hold spares and replace equipment and/or Software in order to conduct a repair, copy the data and perform backups to ensure that no data is lost or corrupted. Any lost data and associated costs of recovery is Supplier's responsibility.
EUC-ES-04	The Supplier shall, wherever possible, support and repair the defective equipment using remote system management tools with which corrective maintenance can be performed on an End User's device in-line with the Customer's Security Process and Policy.
EUC-ES-05	The Supplier shall, in agreement with the Customer, provide approved alternative solutions for End Users (including branch equipment) experiencing an equipment or software Incident to access replacement equipment.
EUC-ES-06	The Supplier shall, provide, in agreement with the Customer, nominated sites to which End Users (including branch equipment) can attend when requiring an equipment or software upgrade, repair or replacement equipment.
EUC-ES-07	The Supplier shall, upon repair of malfunctioning equipment: - (a) return the repaired item to the spares loop; (b) direct to the End User; and (c) or to the appropriate Nominated Office for collection.
EUC-ES-08	The Supplier shall, ensure that 3d barcodes / asset tags and support tags are replaced as applicable on all kit.
EUC-ES-19	The Supplier shall, provide engineering services for the Customer's Production, Pre-Production, and other End User Test Devices, including devices located in Third Party locations.
EUC-ES-10	The Supplier shall, provide on-site support to one defined location and additional part-time support to two defined locations which shall include: (a) floor walkers; and (b) drop in surgeries / Tech bars to support End Users.

6.4.2 Enhanced Engineer Services

The provision of enhanced arrangements for defined VIP Colleagues or Branches.

Req ID	Requirement Description
EUC-EES-01	The Supplier shall, provide a contact number to enable the Customer's support staff to contact the VIP services.
EUC-EES-02	The Supplier shall, provide a solution for VIP Services, which allows for in person and remote engagement, to a number of identified VIP Users which has enhanced SLAs that meet the needs of the Customer's VIPs.
EUC-EES-03	The Supplier shall, as agreed with the Customer, provide enhanced support up to a max. of 50 Colleague VIP users. These services will include but, are not limited to: (a) Incident Management; (b) Request Management;

POL00337657

	(c) Knowledge Share; (d) User Experience; (e) Asset & Configuration Management; (f) Audio Visual (AV); (g) Security support.
EUC-EES-04	The Supplier shall, provide support to VIPs while out of their normal office location including while at their home or in transit.
EUC-EES-05	The Supplier shall, be responsible for assuring any engagement is logged and recorded in the Customer's ITSM tool, on behalf of the VIP user.
EUC-EES-06	The Supplier shall, ensure the details of VIP Users held by the Supplier are kept aligned with the Customer's details within the ITSM tool and Asset Configuration Management records.

6.4.3 Field Engineer Services

Our Field Engineering teams are an important face of the Post Office to the Postmasters, and they should act as brand ambassadors, playing their part in explaining the benefits of the Post Office and its support structure. Field Engineers are seen as a key interface between the corporate head office and the Branch network. Field teams provide a break/fix, support and maintenance service for Branch counter hardware, as well as providing services for Branch opening, changes and closures (See Operational Business Change Process).

In addition to responding to a fault incident, Field Engineers should also provide:

- Support guidance (e.g. use of engagement methods Branch Hub & Service Desk, numbers to call, how to escalate etc).
- Technical guidance (e.g. tips on peripherals such as keyboards, screens brightness settings, how to clean the printer, how to reconnect the scanners).
- Counter hardware support & maintenance.
- Network router connectivity and cabling support.
- Proactive fault reporting and resolution - For example if a Branch raises an incident ticket with regards to a till, and during a field visit, it emerges that a scanner device in the branch is out of service, the field engineer should proactively carry out the necessary administrative tasks to initiate break-fix / replacement (e.g., raising a ticket), and following this carry out the repair task.

Req ID	Requirement Description
EUC-FES-01	The Supplier shall, adhere to Institute of Electrical and Electronics Engineers (IEEE) standards as well as the Customer technical and security policies and guidelines.
EUC-FES-02	The Supplier shall, provide a dedicated field engineering dispatch resource to support the Customer's service desk and support teams for the management and allocation of field engineer workorders and prioritisation of demand.

POL00337657

EUC-FES-03	The Supplier shall, provide Field Engineering Services to ensure: (a) IT equipment is available and optimised; (b) End User compliance and competence in the use of the equipment; (c) End User Branch training; (d) End Users are aware of any ongoing changes to the infrastructure and operating systems.
EUC-FES-04	The Supplier shall, provide a dedicated Engineering and Field Engineering Service Manager to the Customer and provide a monthly service review management report/dashboard and meeting review.
EUC-FES-05	The Supplier shall, ensure that all engineers that visit any Customer site has been DBS checked in line with the Customer's clearance and vetting policy.
EUC-FES-06	The Supplier shall, ensure all engineers that visit any Customer site will comply with the request and directions of the Branch Manager whilst on site.
EUC-FES-07	The Supplier shall, ensure that all engineers details are recorded and maintained on the Customer's database of approved engineers (verification table) used for Branch end users to verify point of entry.
EUC-FES-08	The Supplier shall, coordinate with the Customer's Service Desk, Internal and Third-Party Suppliers to manage all on-site technical support requests to Resolution and Closure within Scope of service.
EUC-FES-09	The Supplier shall, support Branches in remote locations including islands within the UK, Northern Ireland and those with restricted access where arrangements must be made with the End User and consideration made to journey travel times, constraints and opening times.
EUC-FES-10	The Supplier shall, support Branches in Third Party premises where arrangement must be made with the End User and consideration made to access times constraints and minimise disruption to their business operations.
EUC-FES-11	The Supplier shall, support End User environments in domestic locations where arrangement must be made with the End User and in consideration of constraints and working hours.
EUC-FES-12	The Supplier shall, bundle work together by Branch or Geographic area to optimise the schedule ensuring it meets the Customer's SLAs.
EUC-FES-13	The Supplier shall, utilise the Customer's field engineer tooling solution for the deployment, tracking capability and Estimated Time of Arrival (ETA) information for the management and deployment of the Filed Engineering service.
EUC-FES-14	The Supplier shall, ensure that all actions taken during a site visit are recorded in the Customer's ITSM tool prior to the engineer leaving site.
EUC-FES-15	The Supplier shall, as agreed with the Customer, perform planned maintenance on a calendar or condition-based schedule (whichever is appropriate for the asset type).
EUC-FES-16	The Supplier shall, dispatch appropriate trained and equipped field engineers in response to an Incident or Service Request as per ticket priority and timescales defined in Service Level schedule.
EUC-FES-17	The Supplier shall, ensure peripherals deployed in the estate are asset tracked by serial number, location, deployment date and updated in the Customer's ITSM tool.
EUC-FES-18	The Supplier shall, if requested by the Branch Manager or Customer support teams and time permitting, during a site visit, perform counter network and peripheral cabling checks and any necessary remediation actions.

POL00337657

EUC-FES-19	The Supplier shall, if requested by the Branch Manager or Customer support teams, when attending a location undertake a Branch conformance review and functionality checks to maintain availability of the IT equipment and record the outputs within a centralised repository so the Customer can easily access them.
EUC-FES-20	The Supplier shall, be accountable for the management of PCI compliant activities associated with any applicable processes, this includes: (a) providing secure storage for all assets; and (b) delivery and tracking of all assets to branch locations to ensure continual chain of custody.
EUC-FES-21	The Supplier shall, where requested by the Customer, undertake a simple (1 or 2 questions) Customer Satisfaction Engagement Survey with the End Users and provide the results in a consolidated report.
EUC-FES-22	The Supplier shall, provide stock distribution points throughout UK in secure Customer location, Supplier warehouses or alternative solution to aid resolution response times with a focus on remote and very remote locations where achieving Service level are at most risk of breaching.
EUC-FES-23	The Supplier shall, provide the ability for End Users to: (a) receive their devices and/or peripherals at home or work location; and (b) receive or return their devices and/or peripherals via post.
EUC-FES-24	The Supplier shall, be responsible for informing the Customer of any Health & Safety issues relating to any site visits that will prevent the engineer starting, completing or continuing with their allocated workload.
EUC-FES-25	The Supplier shall, ensure that Field Engineering will support the Customer's Branch estate for the installation, checks, removals and replacement of IT cabling: (a) between network equipment and end user hardware; (b) between End User IT hardware; (c) End user IT and 3rd party IT equipment; and (d) Third party IT hardware and network equipment.
EUC-FES-26	The Supplier shall, provide an engineering service at peak periods, or as requested by the Customer, for proactive maintenance visits and enhanced service levels to agreed sites (tbc estimated 50 - 100 sites).
EUC-FES-27	The Supplier shall, during a site visit, provide Support and Technical guidance when requested by the Customer, including: (a) guidance on support engagement methods and escalations; and (b) basic technical guidance including tips on branch devices and peripherals.
EUC-FES-28	The Supplier shall, provide engineering support when requested by the Customer to assist with network connectivity and hardware at Customer sites to include, but not limited to: (a) Router (Inc. WIFI and Cellular); (b) Switches; (c) Hubs; and (d) Cabling.
EUC-FES-29	The Supplier shall, provide proactive fault reporting and resolution where additional faults are identified by the engineer whilst on site responding to an initial Incident raised by the Branch.
EUC-FES-30	The Supplier shall, deliver the Services in line with the Customer's geographical definition of branch locations in the Network Segmentation Report: (a) City & Town; (b) Urban;

POL00337657

	(c) Rural; (d) Remote; (e) Island Exceptions; (f) Outreach; and (e) None customer facing.
EUC-FES-31	The Supplier shall, ensure the Customer has the ability to request a change of location for an individual branch due to circumstance change, mis-categorisation, error or new branch or change of location occurs.
EUC-FES-32	The Supplier shall, ensure the Customer has the ability to change the priority level of a Branch incident resolution level (either up or down) to support business needs or escalation.
EUC-FES-33	The Supplier shall, as agreed with the Customer, maintain defined stock levels for the in-scope hardware.

6.4.4 Stock Management

The process of ordering, storing, tracking, and controlling inventory.

Req ID	Requirement Description
EUC-SKM-01	This requirement is purposely blank.
EUC-SKM-02	The Supplier shall, provide the ability to forward forecast Stock levels required to meet demand based on historical data and other leading indicators.
EUC-SKM-03	The Supplier shall, as agreed with the Customer, maintain defined stock levels for the in-scope hardware
EUC-SKM-04	The Supplier shall, ensure that where it is viable/practicable, assets remain installed in locations for their lifespan to deliver maximum value for money.
EUC-SKM-05	The Supplier shall, proactively identify inactive assets and coordinate the removal or reallocation of such assets with the guidance of the Customer IT security team.
EUC-SKM-06	The Supplier shall, as agreed with the Customer, ensure when hardware is procured from a Third-Party Supplier, they will manage the stock in accordance with this contract.
EUC-SKM-07	The Supplier shall, ensure that all of the End User equipment returned to or from the spares loop is tracked throughout its lifecycle.
EUC-SKM-08	The Supplier shall, provide a monthly report for all items that have been removed from the asset register that are beyond economic repair and seek approval to be decommissioned.
EUC-SKM-09	The Supplier shall, in agreement with the Customer, define and deliver a process for ensuring scrappage, data deletion and decommissioning of all end user equipment, and provide certification of completion.
EUC-SKM-10	The Supplier shall, provide all logistical services (for example, provisioning site preparation etc.) associated with the movement of the equipment or software from Third Party Suppliers.
EUC-SKM-11	The Supplier shall, verify that equipment is stored in a secure area and are not subject to extreme heat, cold, dampness, dirt, etc.

POL00337657

EUC-SKM-12	The Supplier shall, ensure all assets: (a) contain a visible asset identifier, which is robust and visible to the End User which matches the digital identifier; (b) are stored and recorded within the CMDB before the asset is used; and (e) are updated, whenever practicable, to ensure that the asset and configuration record is current.
EUC-SKM-13	The Supplier shall, ensure when any asset loss or theft has been identified inform the Customer immediately outlining the: (a) asset details; (b) value; (c) user information; (d) any data loss or potential risk; (e) the circumstances and investigation; and (f) where applicable and agreed with the Customer , invoke remote wipe as per the Security standards.
EUC-SKM-14	The Supplier shall, as agreed with the Customer, provide a stock report outlining but not limited to the following: (a) usage of branch assets; (b) asset age and end of life (EOL) status; (c) current level of stock required to meet SLA and Operational Business Change needs; (d) details of consumables e.g. cables and PSU for branch devices; (e) PAT testing on receipt of powered equipment; and (f) maintenance / reporting on PAT re-test status.
EUC-SKM-15	The Supplier shall, for each Service Period, produce a disposal report detailing assets disposed of, last user and confirmation of secure data destruction in accordance with security policy and process.
EUC-SKM-16	The Supplier shall, provide secure storage for in scope End User devices which need to be covered by chain of custody for PCI-DSS.
EUC-SKM-17	The Supplier shall, sample check, no more than monthly, all stock inventory to ensure quality whilst held in the Supplier's secure storage.
EUC-SKM-18	The Supplier shall, provide the Customer with a report, no more than monthly or as required by the Customer, detailing the Supplier's stock management information.

6.4.5 Configuration Management

The Process responsible for tracking and reporting the value and ownership of Assets throughout the Contract Lifecycle.

Req ID	Requirement Description
EUC-CONM-01	The Supplier shall, at all times adhere to the Customer's Asset Configuration Management Policies and Processes in the delivery of their Services
EUC-CONM-02	The Supplier shall, be responsible for managing and ensuring the accuracy of their services and components, including mapping of components into services within 1 week of receipt, into the Customer's CMDB.

POL00337657

EUC-CONM-03	The Supplier shall, ensure all assets, licensing and/or Configuration Management information is updated in the Customer CMDB to reflect the changes which have resulted from the installation or movement of assets and initiation of Services.
EUC-CONM-04	The Supplier shall, enable discovery and service mapping access to their estate for the purposes of real-time CMDB population in the Customer's ITSM tool.
EUC-CONM-05	The Supplier shall, as defined by the Customer, ensure that Configuration Items (CIs) are identified in the CMDB by: (a) attributes that describe their functional and physical characteristics; and (b) linked to immutable asset tags.
EUC-CONM-06	The Supplier shall, ensure that Configuration Items are recorded from receipt to disposal, including accurate data within the Customer CMDB tool.
EUC-CONM-07	The Supplier shall, as agreed with the Customer, attend CMDB review and performance meetings, including responding to queries and requests concerning the Configuration Items or supporting information.
EUC-CONM-08	The Supplier shall, if a discrepancy is found with information regarding a Configuration Item, take corrective action to address the discrepancy, including but not limited to: (a) identifying any CIs not recorded in the Customer CMDB or incorrectly recorded by adding or correcting such records; (b) reporting on, updating and removing of assets/CIs that cannot be located; (c) be responsible for any items that can't be located; and (d) taking corrective action if a physical audit identifies any deficiency in the accuracy or completeness of the records in the Customer CMBD.
EUC-CONM-09	The Supplier shall, proactively monitor and resolve the expiry of Configuration Items, including licenses, tokens and assist the Customer and Third-Party Suppliers with keeping the information current.
EUC-CONM-10	The Supplier shall, be responsible for: (a) producing monthly reports that outline a 12-month look ahead to all major software publisher renewals. (b) respond in a timely manner to queries and requests concerning the hardware and software asset inventory data or supporting information; (c) ensure that all deployment of software procured by the Customer or the Supplier is compliant with the number of purchased licenses; and (e) conduct assurance reviews and audits and provide evidence to the Customer and its auditors of the accuracy and completeness of the records in the Customer CMDB and the existence of CIs.

6.5 Build, Software Packaging & Release Management

The Provision, packaging and maintenance of Post Office devices operating systems and corporate applications.

6.5.1 Release and Deployment Management

POL00337657

Hardware, software, documentation, processes or other components required to implement one or more approved Changes to Post Office IT Services.

Req ID	Requirement Description
EUC-RDM-01	The Supplier shall, work with the Customer in defining the delivery of the Release Management process and agree ways of working.
EUC-RDM-02	The Supplier shall, implement documented processes and standards for software and patch deployment procedures which meet requirements and adhere to Customer-defined policies.
EUC-RDM-03	The Supplier shall, design, build, configure, and test all releases in conjunction with the Customer and/or the other Suppliers as necessary.
EUC-RDM-04	The Supplier shall, obtain sign off for the testing approach, testing, UAT and results from the Customer for all releases and deployment.
EUC-RDM-05	The Supplier shall, develop and publish a quarterly release software schedule for in scope assets in alignment with the Customer's standards.
EUC-RDM-06	The Supplier shall, validate that all items being rolled out, or changed, are secured in accordance with the Customer's Information Security Standards and traceable through the Customer CMDB.
EUC-RDM-07	The Supplier shall, resolve all release issues for services within their scope, escalate cross functional issues for resolution, support business deployment acceptance testing and acquire governance sign-off in line with the Customer's Policies and Processes.
EUC-RDM-08	The Supplier shall, establish and maintain software control and distribution procedures, including the management of the software Configuration Items and their distribution and implementation.
EUC-RDM-09	The Supplier shall, support the Customer in their delivery and release impact assessments planning which includes but is not limited to: (a) Security assessments; (b) DR impact; (c) Architectural regression impact and (d) Testing.
EUC-RDM-10	The Supplier shall, maintain and manage the pre-production and test environments for Services, as required, in support of releases.
EUC-RDM-11	The Supplier shall, provide and manage testing for releases before they are transferred to the production environments, including testing of rollback as described by the agreed back-out plans.
EUC-RDM-12	The Supplier shall, review and test changes including, but not limited to, hotfixes, patches, Quality updates, Feature updates and service packs with the Customer's End User hardware builds for compatibility with existing Customer builds/ hardware to ensure that no bugs or issues are introduced as a result.
EUC-RDM-13	The Supplier shall, monitor, assess and test End User Devices (to the appropriate level as agreed with the Customer) patches, hotfixes, Windows updates and service packs, and recommend those which should be applied to improve stability, performance or security.
EUC-RDM-14	The Supplier shall, deploy security patches in accordance with information security recommendations and associated SLAs. Where the Supplier deems that such patches are inappropriate to be delivered within the timeframes specified by the information security team, the Supplier shall notify the Customer and agree a suitable action plan.

POL00337657

EUC-RDM-15	The Supplier shall, advise the Customer of additional vulnerabilities and bug fixes during the ongoing management of the Customer's servers, End User devices and other supported equipment as they become known to the Supplier, including: (a) the means of protecting against these vulnerabilities where known; and (b) applying the agreed protection and any further patches in accordance with the Customer's Change Control Procedure and SLAs.
EUC-RDM-16	The Supplier shall, ensure all builds including Standard server, End User Devices and other support equipment builds contain the agreed patches to protect against known security vulnerabilities and any further patches required by the Customer.
EUC-RDM-17	The Supplier shall, test the updates on the relevant Standard Builds in a test environment.
EUC-RDM-18	The Supplier shall, use where practical, a remote and automated deployment tool to deploy the updates to the Customer's supported equipment.
EUC-RDM-19	The Supplier shall, liaise with the Customer service owner to arrange a suitable time to perform the patch deployment where the Customer's supported equipment is agreed to be excluded from the automated patch management process.
EUC-RDM-20	The Supplier shall, maintain and provide suitable documentation of the patch management process.
EUC-RDM-21	The Supplier shall, prior to full deployment of Third Party-supplied corrections and patches, work with the Customer to pilot and test such corrections to confirm compatibility or special requirements.
EUC-RDM-22	The Supplier shall, prior to each release, produce an overview report outlining code content, objectives, outcomes and risks which shall be reviewed and approved by the Customer in accordance with the Operational Change Process and Policies.
EUC-RDM-23	The Supplier shall, conduct a post deployment review to be provided to the Customer.
EUC-RDM-24	The Supplier shall, document & resolve Incidents and Problems related to software distribution that has failed on End User devices.
EUC-RDM-25	The Supplier shall, prior to distribution, communicate to the Customer's user community any updates on: (a) releases of software and patches; (b) knowledge / support articles; and (c) user training, etc.

6.5.2 Build and Software Update Management

The process of creating, updating and maintaining the standardised build images and approved application list, compiling them into a build artefact.

Req ID	Requirement Description
EUC-BSUM-01	The Supplier shall, be responsible for the secure development, maintenance and support of multiple Client Builds that meets the requirements of the Customer.

POL00337657

EUC-BSUM-02	The Supplier shall, develop a set of standardised images and use the remote Software distribution system to deploy those images to all End User devices.
EUC-BSUM-03	The Supplier shall, securely administer and control in line with the Customer's policies and processes, the distribution and installation of software, in accordance with the relevant software license agreements.
EUC-BSUM-04	The Supplier shall, maintain master copies of the software packages version approved by the Customer in a secure, central location accessible by the Customer.
EUC-BSUM-05	The Supplier shall, be required to ensure that all End User devices provided from the Customer's Service Catalogue are compatible with the Customer's standard build.
EUC-BSUM-06	The Supplier shall, work with Third Parties as required to deliver images installed on all applicable End User devices.
EUC-BSUM-07	The Supplier shall, at a minimum N-1 or as agreed with the Customer and where applicable, test, maintain, and update End User device images to meet the Customer's business requirements.
EUC-BSUM-08	The Supplier shall, continually review Software and End User devices and Configurations of the images for compatibility against current and planned environments and take appropriate action to maintain them in accordance with the Long-Range IT Plan.
EUC-BSUM-09	The Supplier shall, as agreed with the Customer, be responsible for configuring End User devices with personalisation to minimise deployment and engineering times at the Customer's sites.
EUC-BSUM-10	The Supplier shall, on a quarterly basis update the build images with the latest security updates, utilities and software releases prior to an End User device being deployed.
EUC-BSUM-11	The Supplier shall, as agreed with the Customer, ensure that all software and patch deployments follow an agreed maintenance window to reduce the impact on business activities.
EUC-BSUM-12	The Supplier shall, provide input on End User training materials to the Customer for approval as part of the release of each build update.
EUC-BSUM-13	The Supplier shall, be responsible for management of the Customer's cloud-based productivity suite of applications, collaboration services and continual upgrade to latest supported versions.
EUC-BSUM-14	The Supplier shall, ensure that all Client Builds be included in the 'Definitive Media Library (DML)' at a minimum N-1 or as agreed with the Customer.
EUC-BSUM-15	The Supplier shall, where required, make Client Builds available to the Other Suppliers at the request of the Customer.
EUC-BSUM-16	The Supplier shall, define the configuration of each Client Build and provide the configuration document to the Customer.

6.5.3 Equipment and Software Refresh

The cycle of regularly updating key elements of the contracted IT infrastructure to maximize system performance.

POL00337657

Req ID	Requirement Description
EUC-ESR-01	The Supplier shall, be responsible for deploying in-scope agreed equipment and software associated with any refresh and updating the DML in accordance with Customer's Standards.
EUC-ESR-02	The Supplier shall, in agreement with the Customer, refresh the in-scope assets during the Call Off Contract Period including management responsibility for the assets, the implementation, and on-going support.
EUC-ESR-03	The Supplier shall, for in scope assets, be responsible for any obligations to refresh which will include, but is not limited to: (a) provision of personnel who are adequately trained in the use of the equipment or software to be deployed as part of the refresh, and provide such training prior to the refresh; (b) provision of minimal disruption to the Customer's business operations associated with technology refresh; (c) performing all Operational Changes to equipment and software; (d) commercial coverage for third parties if needed; and (e) providing license costs.
EUC-ESR-04	The Supplier shall, provide information regarding the availability of new items of hardware and software available in order to maintain the technology estate in accordance with the Customer's Continuous Improvement Schedule.
EUC-ESR-05	The Supplier shall, work with other Third-Party Suppliers to identify new hardware or software to meet technology refresh needs.
EUC-ESR-06	The Supplier shall, in agreement with the Customer and where applicable, maintain registered software levels at n-1.

6.5.4 Packaging and Software Distribution

This service covers the application code releases in respect of application code fixes or changes developed by Post Office or its third parties. This includes application code fixes or changes in respect to the Horizon branch application and colleague window devices. This includes all element associated with application release management including application packaging, UAT testing and package deployment to till devices in branches.

Req ID	Requirement Description
EUC-PSD-01	The Supplier shall, in adherence to the Customer's change management process, provide secure packaging, associated configuration, sequencing and deployment of all defined software.
EUC-PSD-02	The Supplier shall, ensure all packages can be regressed to the previous working state/last known good configuration and perform regression.
EUC-PSD-03	The Supplier shall, ensure all packages are regression tested against the environment to ensure no conflicts.
EUC-PSD-04	The Supplier shall, investigate and resolve all install failures efficiently through root cause investigation and remediate packages as necessary.
EUC-PSD-05	The Supplier shall, notify the Customer of any updates and upgrades made available by other Suppliers in relation to any software in the scope of the Customer's End User environment where the update or upgrade addresses any issue (Inc. security).
EUC-PSD-06	The Supplier shall, as agreed with the Customer, remediate any packages released before, during or after deployment, deemed not to be fit for purpose during the package lifetime. This will include repackaging, updating or deleting the existing package.

POL00337657

EUC-PSD-07	The Supplier shall, ensure that all deployed packages should be scripted so as to minimise End User intervention including automatic reboots.
EUC-PSD-08	The Supplier shall, in agreement with the Customer be responsible for keeping all software up to date on the Customer's End User environment, including security fixes, patches and software revisions as described in the Technology Framework (section 4 – Technology Framework).
EUC-PSD-09	The Supplier shall, minimise impact on business operations when distributing or installing software.
EUC-PSD-10	The Supplier shall, inform End Users of any reboot required by a software installation and allow users to postpone reboot (within limits agreed with the Customer) other than in an emergency situation.
EUC-PSD-11	The Supplier shall, document and perform Quality Assurance testing of the installation and configuration of the application package including coordinating with the Customer's authorised users for user acceptance testing.
EUC-PSD-12	The Supplier shall, perform application package conflict detection against the Customer's defined core applications and provide resolution and re-packaging, if required.
EUC-PSD-13	The Supplier shall, provide documentation in relation to this service, which includes help files for packages, package knowledge articles and such documentation as required by the Customer.
EUC-PSD-14	The Supplier shall, develop package request forms and documentation templates (e.g. test scripts) pursuant to the Customer's requirements.
EUC-PSD-15	The Supplier shall, ensure that Application Packages and Standard Builds are tested and integrated with other Applications to ensure interoperability.
EUC-PSD-16	The Supplier shall, ensure that no End User data is lost or corrupted as a result of the package installation including business content or configuration data.
EUC-PSD-17	The Supplier shall, provide reporting showing but not limited to: (a) the number of packages successfully installed; (b) those pending; (c) error ratios; and (d) remediation plans.
EUC-PSD-18	The Supplier shall, for Android devices, provide: (a) 3 packaged applications; and (b) 2 app store applications per year, as requested by the Customer.
EUC-PSD-19	The Supplier, shall create application packages, which are ready for deployment within 10 working days from approval, that: (a) automate the installation of Customer's applications; and (b) customise the Customer's configuration requirements and Supplier's standards.

6.5.5 Modern Deployment Management

The process for managing legacy and new applications in a unified way by providing enhanced oversight, security, and awareness.

Req ID	Requirement Description

POL00337657

EUC-MM-01	The Supplier shall, in agreement with the Customer, ensure that the Modern Management Service is capable of delivering multiple builds and operating systems (e.g. Windows 10, iOS and Android).
EUC-MM-02	The Supplier shall, configure and maintain the End Point Manager in compliance with the Customer's policies and processes.
EUC-MM-03	The Supplier shall, in agreement with the Customer, configure and maintain the approved application list within the definitive media library.
EUC-MM-04	The Supplier shall, in agreement with the Customer, configure and maintain the Autopilot profiles.
EUC-MM-05	The Supplier shall, monitor the End Point Manager performance using native Azure technologies.
EUC-MM-06	The Supplier shall, no more than monthly, report on the configuration details of the devices to enable impact assessment for demand.
EUC-MM-07	The Supplier shall, implement and maintain configuration profiles for multiple builds.
EUC-MM-08	The Supplier shall, as agreed with the Customer, ensure all Windows 10 devices are Autopilot ready.
EUC-MM-09	The Supplier shall, as agreed with the Customer, ensure that all devices are registered in End Point Manager to support self-service deployment.
EUC-MM-10	The Supplier shall, manage and administer Microsoft Defender ATP. This includes but is not limited to: (a) management of dashboards; (b) the review and implementation of security recommendations; (c) management and remediation of vulnerabilities; (d) corrective actions to remediate security incidents; and (e) forecast, notify and test (when possible) signature updates before deployment to live.
EUC-MM-11	The Supplier shall, as agreed with the Customer, provide regular End User Devices health reports and take pro-active action on any irregularities or risks highlighted.
EUC-MM-12	The Supplier shall, manage and maintain the Customer's Windows 10, iOS and Android build and policies.
EUC-MM-13	The Supplier shall, implement and maintain the Customer's Azure AD groups used for application access and delivery.
EUC-MM-14	The Supplier shall, as agreed with the Customer, enable and manage the integration of other supported technologies into End Point Manager.
EUC-MM-15	The Supplier shall, manage and administer Endpoint Security suite including but not limited to disk encryption and firewall policies.
EUC-MM-16	The Supplier shall, review and test Feature Updates for compatibility with existing Customer builds and hardware to ensure that no bugs or issues are introduced as a result.
EUC-MM-17	The Supplier shall, as agreed with the Customer, deploy approved Feature Updates to all in scope End User devices.
EUC-MM-18	The Supplier shall, create, manage and deploy mechanisms, such as running scripts on End User devices, to allow for the automation of manual task.
EUC-MM-19	The Supplier shall, support and manage the Customer's conditional access policies and BYOD policies, in line with business requirements. Where the policies do not exist the Supplier shall ensure Industry Best Practice in agreement with the Customer.
EUC-MM-20	The Supplier shall, monitor the active and non-active inventory of devices and provide monthly reports to the Customer.

POL00337657

6.6 Service Management

The Post Office will manage the Supplier in a way consistent with a managed service provider, meaning that the Supplier will have autonomy and decision-making power over its scope, however at the same time Post Office will require visibility of certain low-level aspects of the service.

The Supplier will participate in the Post Office governance of its services by providing reporting packs or utilising the Post Office ServiceNow dashboards and reports and participating in governance and operational forums.

At the same time, Post Office needs to have a level of visibility and audit control over a number of aspects the supplier technology environment, services and activities with regards to assuring that the IT delivery meets the required quality, security and compliance standards. This level of visibility includes governance activities, but also an expectation that the Supplier provides to Post Office a high level of visibility of the operational environment, workflows, controls, right to audit and compliance status information.

Post Office are moving to a more user-centric focus to service delivery, including undertaking user feedback surveys to gauge levels of user satisfaction, and driving remediating issues that are identified by user surveys.

The Supplier is expected to take a proactive approach to service delivery which includes ongoing management of outcomes, discovering the causes of failures, actively bringing about improvement where shortfalls are identified, measuring and managing Customer satisfaction, and providing a continuous improvement approach.

6.6.1 Financial and Contractual Management

Financial control and accountability within the Post Office is split between the Service Management and Contract Management functions. The Post Office Service Manager manages the day to day spend and authorisation of invoices along-side the checks and controls of the Contract Manager.

Req ID	Requirement Description
EUC-FCM-01	The Supplier shall, at all times adhere to the Customer's Financial Management Policies and Processes in the delivery of their Services.
EUC-FCM-02	The Supplier shall, comply with the Customer's requisition, purchase order and invoice management processes and submit financial reports, where requested, by the Customer via the appropriate IT systems.
EUC-FCM-03	The Supplier shall, provide the Customer with any pro-forma invoice for approval, by the Customer, prior to submitting the invoices to the Finance department.

POL00337657

EUC-FCM-04	The Supplier shall, ensure all submitted invoices for Services rendered address any SLA amendments and are accompanied by backing data, in a format agreed with the Customer, to assist the Customer to review and reconcile charges prior to invoice payment.
EUC-FCM-05	The Supplier shall, invoice the Customer, within one calendar month, in arrears for services rendered.
EUC-FCM-06	The Supplier shall, when unable to invoice the Customer within one calendar month, notify the Customer any charges not yet billed and agree to invoice within 6 months of Services rendered. The Customer will not accept any charges older than 6 months from date of service delivered.
EUC-FCM-07	The Supplier shall, cooperate with the Customer to answer any questions, to resolve any invoice or consumption dispute and/or any invoice adjustments that may arise.
EUC-FCM-08	The Supplier shall, assist the Customer in the development and implementation of the consumption reporting and invoicing processes.
EUC-FCM-09	The Supplier shall, provide a consolidated operational spend report (split by business function), of which the format should be agreed with the Customer, of the actual IT costs over agreed periods (at the minimum monthly) to the Customer.
EUC-FCM-10	The Supplier shall, provide a quarterly report on the utilisation of each role on the contracted Rate Card outlining consumption and utilisation of each element.
EUC-FCM-11	The Supplier shall, provide, as agreed with the Customer, a regular monthly statement of account.
EUC-FCM-12	The Supplier shall, create and manage a financial tracking model which includes but, not limited to: (a) contracted commitment with the Supplier by financial year with total contract value agreed as per signed contract; (b) forecast by financial year and by month; (c) actuals and forecast by month for the current financial year that can be reconciled back to monthly invoices; and (d) breakdown of any Contract Management Notes (CMN) over and above the base contract.
EUC-FCM-13	The Supplier shall, as agreed with the Customer, attend a monthly financial review meeting which will include but not limited to: (a) review of the financial tracking model to cover actuals and forecast against contract values; and (b) review of any Purchase Order / Invoice / Billing queries.
EUC-FCM-14	The Supplier shall, as agreed with the Customer, attend a monthly contractual review meeting which will include but not limited to: (a) provide evidence of compliance; (b) agree actions to meet their unmet obligations and identifying key risks for escalation; (c) provide remediation plans and timelines; (d) review contract performance; and (e) review contract change notes.
EUC-FCM-15	The Supplier shall, lead an annual contract conformance exercise signed off by both parties.

6.6.2 Risk and Compliance

POL00337657

The Post Office Process responsible for identifying, assessing and controlling Risks.

Req ID	Requirement Description
EUC-RC-01	The Supplier shall, at all times adhere to the Customer's Risk Management Processes in the delivery of these requirements for their services.
EUC-RC-02	The Supplier shall, achieve and maintain its own accreditation and certification required as specified by the Customer's policies or standards.
EUC-RC-03	The Supplier shall, hold a full risk register detailing all known Risks, likelihood, impacts and mitigation plans to the Suppliers scope of Service.
EUC-RC-04	The Supplier shall, use automated tools, integration or access directly with the Customer's Risk management tools for recording and updating all risks.
EUC-RC-05	The Supplier shall, agree with the Customer the relevant point at which a risk should transfer to the Customer.
EUC-RC-06	The Supplier shall,: (a) notify the Customer of all risks with the associated scope of Services; (b) provide to the Customer details of how all identified risks impact the provision of the Services; (c) provide the Customer with activities/plans/costs and associated timescales to mitigate the risk; (d) execute agreed risk mitigation plans; and (e) advise the Customer of any residual risk.
EUC-RC-07	The Supplier shall, as agreed with the Customer, provide assistance, investigation and remediation (where applicable to the Suppliers scope) to the Customer in the support of risks identified by the Customer or other third parties.
EUC-RC-08	The Supplier shall, provide a monthly report and attend a monthly meeting to review all risks relevant to the services.
EUC-RC-09	The Supplier shall, facilitate the activities of the Customer's staff, auditors or regulators in conducting assurance activities in relation to the design, operation, effectiveness, investigation or audit of any key risk or assurance controls across the provision or management of any Services provided to the Customer.

6.6.3 Service Catalogue & Request Management

Request management within the Post Office follows a standard ITIL process and is fully managed within the Post Office ServiceNow platform. Requests can come from a number of routes within the Post Office, directly from end users via the Service Catalogue or created outside of the catalogue e.g. by the Post Office Service Desk.

The Post Office Service Catalogue is a centralised service catalogue delivered via ServiceNow. Users can request new catalogue items (such as hardware, software), IT services, project requirements, product enhancements, office supplies, or any other business service, all from one end user portal. When an end user has requested a catalogue item the supplier will be provided with a request for processing.

Catalogue items are either pre-approved where no authorisation is needed by a budget holder and are automatically passed to the supplier as a request for fulfilment (e.g. low value items or consumables). For high value items (e.g. laptops) a Post Office representative will authorise the purchase before it is passed to the supplier for fulfilment.

POL00337657

Each item on the Service Catalogue will have a set price/cost, specification and SLA for fulfilment. This sets the expectations for the end user and via ServiceNow will keep the end user updated on the progress of the request.

As the catalogue and requests are delivered via ServiceNow the management of the service will be delivered via the dashboard, performance analytics and data. The supplier will hold regular (monthly) service reviews with Post Office to review supplier performance, opportunities for future items and the standard service management activities.

The current list of related service requests is provided in **Appendix A**: **Ref Doc-006 Service Catalogue v2.0**

Req ID	Requirement Description
EUC-SCRM-01	The Supplier shall, work with the Customer in defining the delivery of the Service Catalogue process and agree ways of working.
EUC-SCRM-02	The Supplier shall, in a format specified by the Customer, provide details of all items and services to be included in the Customer Service Catalogue and ensure that the data is up to date and accurately reflects the items.
EUC-SCRM-03	The Supplier shall, ensure that any changes to catalogue items (including additions, amendments, and deletions) shall be affected in accordance and agreement with the Customer.
EUC-SCRM-04	The Supplier shall, participate in periodic reviews (no more than monthly) of the Service Catalogue to ensure the catalogue is updated and reflects the Business Rules. This review will also include the Supplier: (a) sample checking the catalogue for completeness and accuracy; and (b) conducting test request exercises to validate the Users end to end experience.
EUC-SCRM-05	The Supplier shall, act as a reseller responding to Customer requests for pricing quotes for EUC-related products that are not defined in the Service Catalogue.
EUC-SCRM-06	The Supplier shall, when requested by the Customer, enable the purchasing of stock items in bulk to enable competitive pricing and enhance response times.
EUC-SCRM-07	The Supplier shall, ensure when items are procured via the Service Catalogue, the User is provided with appropriate guidance or instructions in respect of the use of the hardware/software. Such guidance shall include familiarisation, training and post installation hardware configuration.
EUC-SCRM-08	The Supplier shall, be responsible for administering and co-ordinating Requests on an end-to-end basis throughout their lifecycle.
EUC-SCRM-09	The Supplier shall, in a format agreed with the Customer, provide regular status updates including closure to the Requester for the purpose of tracking, managing and closing Requests.
EUC-SCRM-10	The Supplier shall, use the most cost-efficient way of fulfilling the Request in line with Service Levels and Customer needs.
EUC-SCRM-11	The Supplier shall, provide shipping of equipment to and from Customer Locations (Including temporary facilities), as requested by the Customer. This also may include Supply Chain Members or any Third-Party Supplier.

POL00337657

EUC-SCRM-12	The Supplier shall, be responsible for all freight and transportation costs associated with the shipment and receipt of equipment between the Customer, Supplier and equipment manufacturer locations. The Supplier shall, provide the Customer with tracking references and confirmation of delivery.
EUC-SCRM-13	The Supplier shall, provide the Customer with tracking references and confirmation of delivery including: (a) returns where items are defective; (b) damaged on receipt; or (c) no longer required.
EUC-SCRM-14	The Supplier shall, retain full responsibility for all shipped items until confirmation of receipt is received at the end destination and/or by the Requester.
EUC-SCRM-15	The Supplier shall, be responsible for changing the priority of a Request if requested to do so by the Customer.
EUC-SCRM-16	The Supplier shall, be responsible for invoking triage to determine a suitable course of action when Requests cannot be fulfilled or will be fulfilled outside of the agreed timescale and will escalate, as per the agreed process.
EUC-SCRM-17	The Supplier shall, provide a process to support the Customer in the fulfilment of authorised requests that are not covered on the Service Catalogue.
EUC-SCRM-18	The Supplier shall, advise on expected delivery times for Requests and if these times are likely not to be met. The Supplier shall, always advise on any potential or actual issues with the delivery of any Requests as they arise.
EUC-SCRM-19	The Supplier shall, notify the Customer of any financial implications, resulting from the cancellation of a Request, and co-operate with the Customer to minimise any adverse effects.
EUC-SCRM-20	The Supplier shall, provide responses to all request queries to ensure the Requester has clear guidance of resolving the query, without referring the Requester to another party.
EUC-SCRM-21	The Supplier shall, retain overall responsibility for Requests for their services until the Request is closed. The Supplier is responsible for closing fulfilled Request Records following confirmation from the Requester and initiating closure Processes.
EUC-SCRM-22	The Supplier shall, where they have performed closure of the Request in accordance with agreed guidelines, ensure all necessary Data is captured or updated on completion of a Request including updating the CMDB.
EUC-SCRM-23	The Supplier shall, agree with the Customer any variations required to the End User Client Devices and will ensure such variations are applied to the Service Catalogue in accordance with the Customer's Catalogue Management Change Control Process.
EUC-SCRM-24	The Supplier shall, ensure they provide or support services, as listed in the Customer's Service Catalogue which include: (a) hardware and software provision and procurement; (b) JML Services/requests; (c) End User administration activities; (d) business services requests; and (e) requests from Customer's business unit.
EUC-SCRM-25	The Supplier shall, provide a dedicated resource to support the request and Service Catalogue processes and any escalation management for the service.

POL00337657

EUC-COL-SCRM-01	The Supplier shall, where instructed for Equipment which has reached its final staging destination within the End User Estate: (a) liaise with facility staff at the location to coordinate delivery times/dates; (b) minimise disruption to the working environment (e.g. noise or working space); (c) adhere to any and all health and safety advice; (d) ensure the area is left in the same condition when the work is complete; and (e) ensure that facility staff have approved for the contractor to leave the site either during installation or on completion.
EUC-BR-SCRM-01	The Supplier shall, for equipment and/or software which has reached its final staging destination within the Branch Estate and prior to its actual installation include the following: (a) unload, un-crate and/or remove the packaging that was used to ship and contain the product; (b) remove or otherwise arrange for the disposal of all shipping and packaging materials from the Customer's premises in an environmentally responsible manner as agreed with the Customer ; (c) assemble and/or test the product, including assembling a complete or partial configuration, if required by the agreed installation plan; (d) provide the specific configuration required to complete the assembly and/or installation of the equipment and software; (e) use agreed standard Configuration for the underlying type of equipment and/or software for all new equipment and software, unless otherwise approved by the Customer; (f) provide configuration specifications and assembly/test instructions to the Customer , Supply Chain Member or Third-Party Vendor in electronic format and/or paper copy as needed; (g) provide all parts and materials necessary for proper assembly and installation of equipment, software, Services and IT services, unless agreed otherwise with the Customer , Supply Chain Member or any Third Party Vendor; (h) provide all on-site training needed for end user acceptance; (i) coordinate with all Third Party Vendors that are supplying peripheral or ancillary equipment or software; and (j) provide replacement parts/units to remedy out-of-box failures or equipment found inoperable during assembly.

6.6.4 Service Management

The relationship, process and interaction between the Post Office and Supplier in delivery of the contracted services.

Req ID	Requirement Description
EUC-SM-01	The Supplier shall, adhere to the Customer's Supplier governance model for separate Branch and Colleague Services, which will include but not limited to: (a) daily stand up service reviews (b) weekly service line operational meetings (c) monthly service review to cover all aspects of contracted services (d) ad-hoc operational meetings e.g. Major Incident Review; and (e) quarterly service strategy review meeting.

POL00337657

EUC-SM-02	The Supplier shall, record Continual Service Improvement (CSI), via the Customer's ITSM tool, and update (no more than once a week) all records to reflect progress.
EUC-SM-03	The Supplier shall, deliver their services, at a minimum ITIL v3 and adopt the latest ITIL framework, in line with the Customer's processes and policies
EUC-SM-04	The Supplier shall, develop, within 3 months of the baseline data being captured, and maintain thereafter, its own Service Improvement Plans (SIPs) with measurable improvement targets and provide its plans to the Customer for review and acceptance.
EUC-SM-05	The Supplier shall, be responsible for facilitating reviews of Service data to analyse trends, aggravating factors, weaknesses, improvements and changes.
EUC-SM-06	The Supplier shall, collaborate with the Customer to define the Customer satisfaction survey questionnaire.
EUC-SM-07	The Supplier shall, support and analyse End User feedback, via the Customer Satisfaction Process, and incorporate into the Service Improvement plans to reflect actions to address the feedback.
EUC-SM-08	The Supplier shall, in agreement with the Customer, provide dedicated Service Management resources who are accountable for the day to day delivery and performance of the scope of Services.
EUC-SM-09	The Supplier shall, escalate issues in accordance with the escalation procedures approved by the Customer.
EUC-SM-10	The Supplier shall, support the Customer at conferences and other events, where requested to provide ad-hoc engineering support, assistance and technical expertise, including temporary "pop-ups".
EUC-SM-11	The Supplier shall, provide all relevant information (and underlying information) relating to Service Levels, Service Level Targets and Key Performance Indicators for the EUC Services. The Customer have to right to see this data presented at a granular level by type of site, geographic region, and device.
EUC-SM-12	The Supplier shall, where the Customer requests, provide regular information on the Suppliers performance against each SLA in real-time, where possible. Where real time data is not available, the Supplier will provide data as requested and in agreement with the Customer.

6.6.5 Asset Management

The Post Office CMDB and Asset Management process and system maintain a central, up-to-date record of the set of assets that comprise the service and operational environment, for example Branch Point of Sale devices, tablets, Colleague computers and back-end infrastructure.

The Suppliers Configuration Item (CI) data will be integrated into the Post Office consolidated Configuration Management Data Base (CMDB) to maintain the set of relationships between service assets such as the relationships between services and businesses, owners and Branches that devices are assigned to, support teams, Suppliers and assets (often known as 'service maps').

POL00337657

The Post Office CMDB is maturing due to a move to ServiceNow and is constructed to a Post Office CMDB schema which contains a layered hierarchy of elements. The CMDB shall be deemed to be the master CMDB in which the master records are held.

The CMDB assets are updated in the CMDB after every event in the lifecycle of an asset i.e. purchase, issuance, changes, reassignments, retirement and disposal for the CMDB to reflect the current status and assignment of assets at any point in time.

To retain audit and control of the assets there is a need to label all computers, printers and significant devices with an identification number that is stored in the CMDB, thus facilitating the support and management of devices.

For all major Suppliers within the Post Office Supplier base, a systems integration to the CMDB is created in order to periodically feed all CI records to the Post Office CMDB. The contents of the supplier CMDB and CMDB feed to Post Office is defined by the methods, format and structure that are prescribed by Post Office.

Req ID	Requirement Description
EUC-AM-01	The Supplier shall, create an Asset Register of all equipment and provide ongoing maintenance of the register, for software and related IT services. This includes assets owned or leased on behalf of the Customer and held in stock or deployed at Customer sites, Supplier or Third-Party locations.
EUC-AM-02	The Supplier shall, record the individual data elements defined by the Customer for each in scope Asset and record in the Customer's Asset register which will include, but is not limited to: (a) currently allocated employee or End User; (b) asset type; (c) make; (d) model; (e) firmware version; (f) physical location; and (g) PCI compliance needs.
EUC-AM-03	The Supplier shall, at their cost and in agreement with the Customer: (a) provision and maintain End User asset management discovery tools to N-1 software levels; and (b) record the individual data elements defined by the Customer for each in scope Asset.
EUC-AM-04	The Supplier shall, ensure all in scope assets are tracked throughout their lifecycle and record in the Customer asset register.
EUC-AM-05	The Supplier shall, track assets for support including but not limited to: (a) EOL; (b) End of service life; (c) Extended support; and (d) Warranty.
EUC-AM-06	The Supplier shall, produce a periodic (at a minimum monthly) asset report detailing, but not limited to: (a) the current estate deployment; (b) all assets in storage or spares loops; (c) all software installed on assets; and (d) asset usage trends including last logged in user to know which user is using a particular asset.

POL00337657

EUC-AM-07	The Supplier shall, provide a Definitive Media Library (DML) which includes but not limited to: (a) licensing and cost information; (b) application ownership; (c) deployment instructions; (d) compatibility; and (e) support.

6.6.6 Controls and Best Practice

The Post Office control framework organises and categorises our internal controls, which are practices and procedures established to create business value and minimize risk.

Req ID	Requirement Description
EUC-CBP-01	The Supplier shall, adhere to COBIT 5 including submitting evidence into the Customer controls application on a monthly basis or as defined by the control requirement.
EUC-CBP-02	The Supplier shall, nominate a dedicated resource who shall act as a single point of contact and also be responsible for the management of Control adherence for the Supplier.
EUC-CBP-03	The Supplier shall, produce (where applicable), maintain and improve, no more than annually, all processes and procedures used in delivering the services to the Customer.
EUC-CBP-04	The Supplier shall, when requested by the Customer, support the Customer in defining policy and process using their industry knowledge and best practices.
EUC-CBP-05	The Suppler shall, define and implement remediation actions where specified controls are found to not be effectively implemented.
EUC-CBP-06	The Suppler shall, sample check 10% of controls on a monthly basis with the Customer to ensure that submissions, evidence and responses are appropriate and correct.

6.7 Service Operations

The Post Office Service Desk is the universal service front-end for users, serving the user community of the Branches and Colleague business unit.

The Post Office Service Desk captures work items from end-users, logs the work items into the ServiceNow tool, and applies an initial prioritisation level to the work items (e.g. incident priority).

The Post Office Service Desk manages the first line support, which includes the provision and management of knowledge articles, training and support for end users. The EUC Supplier is there to support the 1st line service desk in resolving on first contact or when a ticket has been escalated through the support model to provide engineering support to resolve the ticket as part of a standard operating model:

- 1st line – The Service Desk provided by Post Office
- Field Engineering – Provided by supplier
- 2nd/ 3rd Line Support – Remote support, provided by supplier for the remediation of escalated incidents

POL00337657

The Service Operations service includes the provision of knowledge articles, training and support for the 1st line Service Desk to resolve on first contact or escalate through the support model.

Right to left shift: The supplier must attempt to empower the Post Office Service Desk to perform first-time fix by providing training, knowledgebase articles and assistance as required.

6.7.1 Incident Management

The Post Office process between the Post Office Service Desk and supplier resolver groups for the resolution of Incidents to return the IT Service to normal for End Users as quickly as possible.

Req ID	Requirement Description
EUC-IM-01	The Supplier shall, at all times adhere to the Customer's Incident Management, IT Security Incident Management and Major Incident Management Processes in the delivery of their Services.
EUC-IM-02	The Supplier shall, utilise and update the ticket or task with all relevant information, (adhering to Customer's Information Security Standards and guidelines) relating to each Incident, including the impact of the incident, actions being taken to resolve and estimated time to resolution.
EUC-IM-03	The Supplier shall, escalate issues to the appropriate levels for resolution in accordance with all agreed escalation procedures, including Security escalation procedures, and in line with all SLAs.
EUC-IM-04	The Supplier shall, manage communication with End Users in respect of Incident status and resolution and ensure that reasons for information supplied to the End User are recorded in the Customer's ITSM Tool.
EUC-IM-05	The Supplier shall, be responsible for liaising with End Users to diagnose and troubleshoot resolution of incidents.
EUC-IM-06	The Supplier shall, where appropriate, ensure where Incidents relate to assets the Incident is linked to the affected CI's within the Customer CMDB.
EUC-IM-07	The Supplier shall, be responsible for supporting the Customer in classifying and determining IT and Cyber Operations Incident categories, impact and urgency. Incident Priority will be based on agreed impact and urgency measures in accordance with Service Levels.
EUC-IM-08	The Supplier shall, for all major incidents, provide prompt notification via an incident ticket within the Customer ITSM tool and a physical communication to the 1st line Service desk or incident management team in line with SLAs.
EUC-IM-09	The Supplier shall, provide the relevant technical resource to be available to attend meetings with the Customer and Other Suppliers, in support of cross functional activities as required to diagnose escalated incidents, Major Incidents and post incident activities.
EUC-IM-10	The Supplier shall, restore the Service as quickly and efficiently as possible, utilising temporary workarounds where appropriate, to the required Service Levels while minimising any adverse Impact on the Customer's business operations.

POL00337657

EUC-IM-11	The Supplier shall, coordinate with the Customer to open new or update existing Problem Management records, where new workarounds are applied to resolve an incident, and ensure that knowledge articles are updated.
EUC-IM-12	The Supplier shall, conduct necessary tests to ensure that an incident is resolved and log the details to confirm resolution of Incident.
EUC-IM-13	The Supplier shall, inform the Customer, via an agreed escalation path, if Incidents exceed, or, are expected to exceed their Target Resolution Times.
EUC-IM-14	The Supplier shall, provide a solution to enable 1st Line support services to contact the Suppliers SME/2nd Line support to facilitate 1st contact resolution via multiple channels, including web chat.
EUC-IM-15	The Supplier shall, take responsibility and ownership for all incidents raised and resolve them in line with the appropriate Service Levels.
EUC-IM-16	The Supplier shall, use all reasonable endeavours to contact the End User when an incident has been assigned for resolution.
EUC-IM-17	The Supplier shall, be responsible for coordinating and managing any required revisits for failed changes within 24hr of receiving the failure notification from the Customer.
EUC-IM-18	The Supplier shall, in agreement with the Customer, manage and control a list of VIP users, applications & branches to reflect the business criticality and appropriate SLA response.
EUC-IM-19	The Supplier shall, in agreement with the Customer, support the initial population and ongoing management of the Incident Matrix which will define the criticality and appropriate SLA for all incident types the Supplier shall be accountable for.

6.7.2 Problem Management

The Problem Management process is to support the Post Office to determine the root cause of error conditions that fall within the wider Post Office Service and the EUC remit. Post Office is considered to be the process owner of the Problem Management process and therefore performs central ownership and decision making around problems, including delegating tasks such as Route Cause Analysis (RCA) report production to Suppliers.

Problem records will be created for P1 and P2 Incidents and Root Cause analysis reporting with regard to these problem records will be undertaken. For recurring lower severity incidents, the supplier is expected to perform its own investigation or support Problems that have originated from the Post Office or other supply chain members. These will be managed as part of the engagement with the Post Office Service Management or Operational teams.

The supplier will need a high degree of technical capability such that deep-dive type investigations into issues such as investigations into platforms and software may be carried out, which can include investigating Windows event logs, machine boot sequences, operating system configurations, operating system files and software log file investigation.

Where a problem has been identified and workarounds put in place, Knowledge Articles and training will be created for the Post Office Service Desk and the EUC Supplier's own support teams where possible, pending the full investigation of a problem and associated remediation work.

POL00337657

The problem process may generate work items to be carried out in order to remediate the root cause issues. In line with the requirement below the EUC Supplier will be required to log, and track actions resulting from Problems and progress the actions through the appropriate forums and tooling.

As with ITIL best practice the EUC Supplier is required to carry out a Proactive Problem Management approach in order to implement measures to prevent issues from occurring in the future and support the shift left approach for the Post Office Service Desk for decreasing contacts and end user impact.

Req ID	Requirement Description
EUC-PM-01	The Supplier shall, adhere the Customer's Problem Management Policies and Processes in the delivery of the Services they are providing the Customer.
EUC-PM-02	The Supplier shall, provide a nominated Problem Management resource to coordinate and support the Customer in the delivery of the service.
EUC-PM-03	The Supplier shall, retain overall responsibility for all problems or tasks allocated to them until the problem or task is closed.
EUC-PM-04	The Supplier shall, as agreed with the Customer, review Incidents to: (a) identify Incident trends or patterns and develop remedial plans; (b) identify single point of failure from incidents and propose remedial plans; (c) provide proactive analysis identifying faults that may lead to incidents; (d) undertake regular reviews of incident management performance and root cause analysis information to identify preventative measures to reduce the frequency of incidents; and (e) implement preventative measures.
EUC-PM-05	The Supplier shall, provide to the Customer an initial route cause assessment report within 24hrs of a Major Incident.
EUC-PM-06	The Supplier shall, create a problem record and document the root cause of the problem and associate incidents, relevant CIs within the known error record.
EUC-PM-07	The Supplier shall, be responsible for updating and reviewing the Service Knowledge Management System (SKMS) and Known Error Database (KEDB) for Known Errors and workarounds.
EUC-PM-08	The Supplier shall, keep the KEDB updated with all incidents that have occurred and have fixes and/or workarounds.
EUC-PM-09	The Supplier shall, ensure the documented Root Cause Analysis (RCA) is completed to agreed standards and timelines which comply with the outcomes specified within the Customer's Problem Management Policies and Process. Where there is a need for further information the Supplier shall be responsible for providing any additional information and include this within the RCA.
EUC-PM-10	The Supplier shall, work with the Customer and any of the other suppliers to assist in the identification, investigation and resolution of Incidents, Problems and Known Errors and the delivery of Root Cause Analysis.
EUC-PM-11	The Supplier shall, implement, in agreement with the Customer, recommendations arising from Root Cause Analysis.
EUC-PM-12	The Supplier shall, be responsible for ensuring Problem Records are updated with the Problem investigation and possible solutions.
EUC-PM-13	The Supplier shall, be responsible, in collaboration with the Customer, for identifying if the solution agreed to the Problem is a workaround or a permanent fix.

POL00337657

EUC-PM-14	The Supplier shall, for in scope Services, proactively identify components that are susceptible to failure, and provide the Customer alternative or remediation plans for resolution and approval. Any remediation actions will be deployed at the Suppliers expense unless in agreement with the Customer.
EUC-PM-15	The Supplier shall, verify with the Customer that a problem is resolved before recommending it for closure.
EUC-PM-16	The Supplier shall, perform Root Cause Analysis on all Priority 1 and Priority 2 Incidents, in respect of Incidents assigned to them and report their findings to the Customer in line with SLAs.

6.7.3 Service Integration

The End-To-End delivery of services across multiple Suppliers and systems

Req ID	Requirement Description
EUC-SI-01	The Supplier shall, for each financial year, work with the Customer to define and agree the licence needs for the use of the Customer's tooling solutions for the delivery of the contracted Services.
EUC-SI-02	The Supplier shall, up to twice a year and in line with ServiceNow releases participate and execute associated regression and integration testing during upgrades.
EUC-SI-03	The Supplier shall, in agreement with the Customer , configure Single Sign On (SSO) for access to MS Office 365 Suite and other federated applications where: (a) such access originates from devices authenticated by the Corporate Identity Services or Collaboration Toolset directory; or (b) such access originates from devices connected via a Secure RAS or LAN Services.

6.7.4 Knowledge Management

To enable an end-to-end integrated service the Post Office and EUC Supplier will require the sharing and creation of knowledge for the purpose of providing a reference knowledge to itself and Post Office support, operational teams and the end users in order to facilitate support, administration and management of the technology environment.

To deliver the services they will need to be documented in the form of IT architecture documents, processes and procedure documents, work instructions, training documents and knowledge base (Kb) articles to facilitate day-to-day support. The service is delivered from the Post Office ServiceNow tool for the purpose of document management, including the document repository and a corresponding management system in order to ensure the production, and continued validation of documentation.

In order to deliver and maintain the Services for its staff and the Post Office Operational and Support teams there is a need for the supplier to provide Post Office Business training for new change to services and ensure that the Service Desk Kb is up to date and accurate. The Post Office have a dedicated Knowledge Manager in support of the Service Desk and Operational team and the Supplier will be expected to regularly liaise with the Manager to review feedback, check compliance and support the general improvement of the service.

POL00337657

The Post Office has invested in the Branch and Colleague self-serve solution which includes the provision of end user knowledge and training articles, videos and other digital communication channels to end users.

Req ID	Requirement Description
EUC-KM-01	The Supplier shall, work with the Customer in defining the delivery of the Knowledge Management process and agree ways of working.
EUC-KM-02	The Supplier shall, update the Service Knowledge Management System (SKMS) immediately as new knowledge articles, FAQs and other assets are produced, or existing knowledge updated.
EUC-KM-03	The Supplier shall, conduct regular assurance activities to ensure information required to manage the Services is captured, stored, and presented accurately and completely in the Service Knowledge Management System (SKMS).
EUC-KM-04	The Supplier shall, develop and maintain new instructions, detailed guidance, FAQs and training materials in response to any changes to the Services and make such instructions, guidance and training materials available.
EUC-KM-05	The Supplier shall, work with the Customer in defining the Tone of Voice process and agree ways of working in the creation of knowledge articles and will submit to the Customer for approval before any article is published, unless in agreement with the Customer.
EUC-KM-06	The Supplier shall, when requested by the Customer, respond to any questions raised via the ITSM Portal and/or update any Knowledge Articles.
EUC-KM-07	The Supplier shall, create, as agreed with the Customer, videos and other media content, Knowledge and Self-Help articles that will be uploaded to the Customer's platform.
EUC-KM-08	The Supplier shall, ensure that its resources involved in creating and maintain Knowledge are sufficiently skilled in the relevant communication techniques to create engaging and easily understandable content relevant to the target audience e.g. technical, End User etc.

6.7.5 Service Operations Change Management

Change Management within Post Office has a central control function across all supplier and clients within the Post Office IT eco system. All suppliers follow and adhere to the single Post Office process and definitions and the EUC Supplier will manage planned IT changes carried out in their technology environment which may impact technology or business operations.

The Post Office Change Management process is delivered in line with ITIL best practice and the EUC Supplier will be required to define, input, manage and progress Request for Change (RFC) tickets to completion which are either generated from their own environments or impacted from external RFCs. Post Office Change Management act as a point of assistance, validation and control to the EUC Supplier change activities and will define the correct change type for changes.

As part of the process the EUC Supplier will attend Post office Change Advisory Board (CAB) meetings in respect of Significant and Major Change types and participate in the impact assessments for all RFCs raised in the CAB.

Change types: The table below provides details of the Change types used in Post Office with the corresponding lead timed and approval requirements:

POL00337657

Type	Lead time	Approval Requirements
Standard	N/A	Preapproved change
Minor	1 day	Ticket electronic approvals only
Significant	5 day	CAB attendance required
Major	10 day	CAB attendance required
Emergency	Immediate	For P1/ P2 incidents. Approval provided via Major Incident call

Table 16: *Change Types*

Req ID	Requirement Description
EUC-SOCM-01	The Supplier shall, at all times adhere to the Customer's Operational Change Management Policies and Processes in the delivery of their Services.
EUC-SOCM-02	The Supplier shall, where required, cooperate with the Customer, other suppliers and designated representatives to minimise disruption of normal business processes and proper receipt of the Services.
EUC-SOCM-03	The Supplier shall, retain overall responsibility for all Operational Changes allocated to them until the Operational Change is closed.
EUC-SOCM-04	The Supplier shall, attend the Customer's Change Advisory Board (CAB) meetings in respect of Significant and Major Change types and participate in the impact assessments for all Request for Change (RFC) raised in the CAB.
EUC-SOCM-05	The Supplier shall, collaborate in the operation of the Customer's Change Advisory Board (CAB) for changes that are not just their own but may impact their services by providing input including: (a) evaluations of change impact; (b) recommendations for approval or otherwise; (c) recommending steps within implementation plans; (d) recommending appropriate participation; and (e) recommending any security concerns or impacts.
EUC-SOCM-06	The Supplier shall, assess the impact, costs, benefit and risk to the Services of the proposed Changes and document the results in the Request for Change.
EUC-SOCM-07	The Supplier shall, identify the impacted Configuration Items set out in the Customer CMDB and associate the Operational Change Record to the relevant configuration items.
EUC-SOCM-08	The Supplier shall, manage the effective entry of Operational Request for Change Records into the Customer's ITSM Tool, including, the correlation of associated incidents, problems and known errors.
EUC-SOCM-09	The Supplier shall, update all operational and other documentation affected by the Change, including any design documentation and Knowledge Articles.
EUC-SOCM-10	The Supplier shall, after implementation of a change, provide feedback regarding actual performance and functionality checks of the Service versus the acceptance criteria.
EUC-SOCM-11	The Supplier shall, support post implementation reviews of Operational Changes to identify opportunities for improvement.
EUC-SOCM-12	The Supplier shall, support joint reviews of any Operational Change failure so that the root causes of post-Operational Change issues can be identified, in addition, the Supplier shall implement any improvements required to prevent a recurrence.

POL00337657

EUC-SOCM-13	The Supplier shall, ensure that any change which results in an Issue, has an Incident raised for it and is linked to the change record in the Customer's ITSM tool.
EUC-SOCM-14	The Supplier shall, provide testing for all change implementation plans as set out in the relevant Operational Change before they are transferred to the production environments including testing of rollback as described by the agreed back-out plans.
EUC-SOCM-15	The Supplier shall, after consultation and as instructed by the Customer, adhere to any changes following any updates/changes to the Customer's Policies and Processes.
EUC-SOCM-16	The Supplier shall, participate in monthly ServiceNow patching and execute associated regression Integration Testing.

6.7.6 IT Service Continuity Management

IT Service Continuity management (ITSCM) ensures that the required EUC IT technical and service capabilities can be resumed within required and agreed business timescales.

The Supplier is required to delivery ITSCM services pursuant to **RM3804-Alternative-and-additional-tc-v4, Schedule B1 Business Continuity and Disaster Recovery**, and in addition the requirements defined below:

Req ID	Requirement Description
EUC-ITSCM-01	The Supplier shall, at all times adhere to the Customer's IT Service Continuity Policies and Processes in the delivery of their Services.
EUC-ITSCM-02	The Supplier shall, ensure their Business Continuity and Disaster Recovery (BCDR) Plan and procedures comply with the Customer's Data Retention Policies and Processes.
EUC-ITSCM-03	The Supplier shall, proactively work with other suppliers as one team to ensure the Customer can integrate the Supplier's IT Service Continuity Plans, with other service providers who deliver Services to the Customer, such that an integrated end-to-end IT Service Continuity Plan can be produced.
EUC-ITSCM-04	The Supplier shall, provide the Customer with a formal report of the business Continuity test results within five (5) Working Days of each test. At a minimum, these reports shall include: (a) the results achieved; (b) any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; (c) measures of performance as compared with normal production performance; (d) a comparison of the results to the measures and goals identified in the respective Continuity Plan; (e) feedback from Users as to the adequacy of continuity for their respective areas; and (f) The Supplier's plan and a schedule to remedy any gaps revealed during testing, to include any User feedback collated by the customer and made available to the Supplier that is applicable to the Services.
EUC-ITSCM-05	The Supplier shall, in agreement with the Customer, ensure all Service Continuity test planning will be designed to minimise business impact and outages.

POL00337657

EUC-ITSCM-06	The Supplier shall, declare disasters in accordance with procedures agreed with the Customer (documented in the BCDR Plan) and notify the Customer of situations that may escalate to disasters as soon as reasonably possible.
EUC-ITSCM-07	The Supplier shall, where services are being backed up, implement controls to ensure viable backups and corresponding records can be used to restore services to agreed levels. The Supplier shall also ensure that back-ups are full, complete and confirm the results of restoring from backups.
EUC-ITSCM-08	The Supplier shall, create and maintain backups, file recovery capabilities and historical archive of files, data and Software (including, where applicable, object code) utilised to process data which are consistent with meeting the Customer's recovery objectives to agreed levels in respect of time and with minimum data loss.
EUC-ITSCM-09	The Supplier shall, ensure that backups adhere to best IT Security standards, such as Encryption at Rest and in line with Ransomware Data Recovery methodologies.
EUC-ITSCM-10	The Supplier shall, in agreement with the Customer, ensure that all Backups are tested and provide a report detailing the test results. Backup tests shall include the ability for the Customer to request sample file restore tests.
EUC-ITSCM-11	The Supplier shall, following any disaster, conduct a post-disaster meeting with the Customer as soon as reasonably possible, in order to understand the cause of the disaster, approve actions to restore the Services to pre-disaster Service Levels (if necessary) and agree actions to develop and implement plans to eliminate or mitigate future occurrences.

6.8 End User IMACD

Provision, packaging and maintenance of Post Office devices operating systems and corporate applications.

6.8.1 End User Services

The provision of IT core build functionality to end users.

Req ID	Requirement Description
EUC-EUS-01	The Supplier shall, provide and support a managed O365 Productivity Platform, including a SharePoint Service site creation, management of templates, restore and export services.
EUC-EUS-02	The Supplier shall, provide support and management of the services within the Customer's Technology Framework (Section 4 Technology Framework), which include but not limited to: (a) capacity management; (b) access management; (c) monitoring and alerting; (d) troubleshooting; (e) setup and ongoing configuration; (f) continuous service improvement and optimisation; and (g) compliance and security.
EUC-EUS-03	The Supplier shall, manage the environment for email accounts that are not directly connected to a single End User.
EUC-EUS-04	The Supplier shall, provide End Users with a capability to access email over the internet that meets baseline minimum best practices and the Customer's standards for encryption in transit and non-repudiation.

POL00337657

EUC-EUS-05	The Supplier shall, provide maintenance and support, through detailed instructions and guidance, to enable End Users to use the archive and retrieve facility.
EUC-EUS-06	The Supplier shall, enable retrieval of all data and/or associated materials and documentation to support forensic examination for the Customer security purposes.
EUC-EUS-07	The Supplier shall, provide support and maintain software for all End Users to enable access to the Customer overall Unified Communications services.
EUC-EUS-08	The Supplier shall, ensure that all automated local data encryption is enabled for all End User Devices including mobile and remote Users.
EUC-EUS-09	This requirement is purposely blank.
EUC-EUS-10	This requirement is purposely blank.
EUC-EUS-11	The Supplier shall, provision login facilities and any necessary Customer software to allow secure access to the Customer's business systems.
EUC-EUS-12	The Supplier shall, provide each End User with at least one unique account, unless agreed otherwise with the Customer.
EUC-EUS-13	The Supplier shall, provide the Customer for each monthly Service Period, information on the number of accounts with no activity in the previous Service Period. The format of the information shall be agreed between the Supplier and the Customer.
EUC-EUS-14	The Supplier shall, implement audit facilities and provide management information which includes but is not limited to: - (a) messaging transmission patterns and profiles; and (b) source and destination journaling of transmitted messages.
EUC-EUS-15	The Supplier shall, configure the End User Devices so that they are provided with a cache of the End User's mailbox to enable the End User to work when their End User Device is not connected to a network.
EUC-EUS-16	The Supplier shall, configure and support the Customer's Corporate Voice and Video Conferencing Service to provide End Users with the capability to hold voice and video conferences.
EUC-EUS-17	The Supplier shall, manage and maintain access to MS Office 365 Suite from Client Devices through Client Software including Internet browsers.
EUC-EUS-18	The Supplier shall, enable multi-factor authentication (MFA) access to the MS Office 365 Suite, except where: (a) such access originates from devices authenticated by the Corporate Identity Services or Collaboration Toolset directory; and (b) such access originates from devices connecting via the Secure RAS or LAN Services (unless otherwise agreed with the Customer).
EUC-EUS-19	The Supplier shall, review and test changes including, but not limited to, hotfixes, patches, Quality updates, Feature updates and service packs with the Customer's End User hardware builds for compatibility with existing Customer builds/ hardware to ensure that no bugs or issues are introduced as a result.
EUC-EUS-20	The Supplier shall, provide End User Device builds incorporating hardware drivers and Software as defined in the Technology Framework (Section 4 – Technology Framework).
EUC-EUS-21	The Supplier shall, in conjunction with the Customer, seek to ensure that all End User Devices meet required local storage requirements and report to the Customer where required local storage requirements are not met.

POL00337657

EUC-EUS-22	The Supplier shall, maintain log on scripts/log off scripts and start-up and shut-down scripts that enable defined End User Device behaviours and controls.
EUC-EUS-23	The Supplier shall, maintain and refresh operating systems and core build software, so they remain under manufacturers' standard support, unless otherwise agreed with the Customer.
EUC-EUS-24	The Supplier shall, monitor, assess and test End User Devices (to the appropriate level as agreed with the Customer) patches, hotfixes, Windows updates and service packs, and recommend those which should be applied to improve stability, performance or security.
EUC-EUS-25	The Supplier shall, develop, test and maintain End User Device builds in such a way that facilitates self-service deployment.
EUC-EUS-26	The Supplier shall, use reasonable efforts, as agreed with the Customer, to continue to support software even where the Software has reached end of life.
EUC-EUS-27	The Supplier shall, provide the facility for all End Users to access web-based applications, through standard browsers that meet the Customer security requirements, supporting common industry standard plug-ins.

6.8.2 End User IMACD

The process for the Installation, moves, additions, changes and deletions to end user equipment, hardware and software.

Req ID	Requirement Description
EUC-IMACD-01	The Supplier shall, plan, schedule and undertake IMACDs in accordance with the Customer Request Fulfilment Process and Change Management Process within agreed timescales.
EUC-IMACD-02	The Supplier shall, ensure that all relevant databases / systems are updated where an IMACD relates to an End User Joiners Movers Leavers (JML).
EUC-IMACD-03	The Supplier shall, agree and implement a process with the Customer by which removable media may be sent for secure disposal.
EUC-IMACD-04	The Supplier shall, undertake and co-ordinate all installations, de-installations, moves, additions, refurbishments and changes for the Customer's End User Environment, and related End User Services at Customer sites.
EUC-IMACD-05	The Supplier shall, provide remote provisioning, support for new or changed devices delivered to remote users.
EUC-IMACD-06	The Supplier shall, create and document the procedures to enable IMACD execution in line with the Customer's Policies and Processes.
EUC-IMACD-07	The Supplier shall, where required, conduct Customer Site surveys to determine the location(s) of the IMACD and any special requirements at the location(s).
EUC-IMACD-08	The Supplier shall, ensure that cabling is provided and connected from the device to the network outlet where applicable.
EUC-IMACD-09	The Supplier shall, define a standard test and success criteria for Customer agreement and approval in the delivery of IMACDs.

POL00337657

EUC-IMACD-10	The Supplier shall, provide guidance, as appropriate, to the End User(s) receiving the IMACD.
EUC-IMACD-11	The Supplier shall, as agreed with the Customer, perform IMACDs for Supplier Personnel.
EUC-IMACD-12	The Supplier shall, on request, de-install and, remove any assets used in the provision of the Services. Following removal, any assets or items which cannot be re-deployed must be disposed of in respect of sustainability, IT Security, health and safety and the Waste Electrical and Electronic Equipment (WEEE) Regulations.
EUC-IMACD-13	The Supplier shall, securely erase all Customer Data on un-installed assets when taken out of service, or where being re-allocated, in accordance with the Customer's Document Retention and Disposal Policy.
EUC-IMACD-14	The Supplier shall, promptly confirm to the Customer, as appropriate, that all equipment, software, parts, cabling, or any other services necessary to execute the IMACD will be available as of the date(s) scheduled for the IMACD.
EUC-IMACD-15	The Supplier shall, promptly confirm the new and/or existing Configuration of the equipment and software associated with the IMACD.
EUC-IMACD-16	The Supplier shall, test the equipment, software, and related Services after the implementation of the IMACD, to include testing in relation to network access.

6.8.3 Joiners, Movers and Leavers:

The Post Office has a diverse and sizable technology estate, where many systems operate shared authentication and authorisation systems. There are several user management approaches in use, which means account management when staff and contractors join, change roles, or leave the organisation is centralised through our Microsoft Identity Management (MIM) solution. This ensures all the processes that drive our joiners, movers and leavers activities are more resilient with clearly defined roles and responsibilities, supported via HR policies & guidance. The supplier as part of the hosting solution of MIM and will also provide a request service for supporting the administration of JML via the MIM solution.

Req ID	Requirement Description
EUC-JML-01	The Supplier shall, monitor, support and maintain the Customer's Joiners, Movers and Leavers (JML) infrastructure solution and integration feeds for both production and non-production environments.
EUC-JML-02	The Supplier shall, on request from the Customer, access and administer non-automated requests via the JML portal.
EUC-JML-03	The Supplier shall, monitor and resolve any file transfer, access, errors or processing issues related to the data feeds.
EUC-JML-04	The Supplier shall, ensure the integrity of the data within the JML systems and support the Customer's data owners in resolving issues or potential issues.
EUC-JML-01	The Supplier shall, monitor and maintain the Customer's Joiners, Movers and Levers (JML) infrastructure solution and integration feeds for both production and non-production environments.

6.8.4 Peripherals:

POL00337657

The supply and management of auxiliary IT devices.

Req ID	Requirement Description
EUC-PH-01	The Supplier shall, in agreement with the Customer, procure a selection of peripherals which will be available to request via the service catalogue.
EUC-PH-02	The Supplier shall, ensure the peripherals supplied meet Customer's security requirements and have the best balance of cost versus user experience.
EUC-PH-03	The Supplier shall, ensure that peripheral and ancillary devices which are contained within the Service Catalogue are supported and compatible with all End User equipment.
EUC-PH-04	The Supplier shall, integrate peripheral equipment with End User Devices and Customer Builds as required to ensure that they are fully functional.
EUC-PH-05	The Supplier shall, where the Customer, Supplier or Third-Party Suppliers identify that peripheral equipment is no longer capable of delivering the Services, will advise and propose alternative peripheral equipment to the Customer.

6.8.5 Print Services:

The enablement for end users to access the services offered by the Post Office Managed Print Services provider.

Req ID	Requirement Description
EUC-PS-01	The Supplier shall, work with other Third Parties to ensure: (a) network connectivity to enable the end-to-end printing solution; and (b) maintain printer integration for all applicable End User devices.
EUC-PS-02	The Supplier shall, work with other Third Parties to ensure network connectivity to enable the end-to-end printing solution
EUC-PS-03	The Supplier shall, identify, prepare, test, distribute, manage, maintain and provide user support for the required drivers for the range of directly attached printers and scanners issued by the Supplier on behalf of the Customer.

6.8.6 Repair and Maintenance:

The process and interactions for the repair and replacement of IT assets

Req ID	Requirement Description
EUC-RM-01	The Supplier shall, as agreed with the Customer, provide warranty repair services for the in-scope End User devices which are in warranty.
EUC-RM-02	The Supplier shall, as agreed with the Customer, provide an out-of-warranty repair service for the list of in-scope End User devices which are out of warranty.
EUC-RM-03	The Supplier shall, provide a temporary like for like replacement for any in-scope End User Colleague devices that are taken for repair.

POL00337657

EUC-RM-04	The Supplier shall, on a timescale agreed with the Customer, advise of any components that are coming to end of life and recommend an alternative component/model.
EUC-RM-05	The Supplier shall, ensure routine maintenance, calendar based, or usage based is maintained in line with manufacturer recommended preventative maintenance.

6.8.7 Accessibility:

The Post Office process for ensuring its current and future IT can be used effectively by everyone, including individuals with disabilities including in Branches.

Req ID	Requirement Description
EUC-ADS-01	The Supplier shall, comply with all relevant Customer Policies, including Security Policies, Processes and relevant external legislation in the relevant jurisdiction, by ensuring all Services, including all associated guidance and communications, are accessible and usable, including those requiring the use of assistive technology.
EUC-ADS-02	The Supplier shall, provide additional support to End Users, including configuration of equipment and /or software to meet the specific needs of the User following receipt of a request via the Services Catalogue.
EUC-ADS-03	The Supplier shall, provide secure End User Device services and support for Accessibility Solutions in the manner that best meets the User's needs in any Site, or, where required, in the User's home.
EUC-ADS-04	The Supplier shall, where requested by the Customer, perform an Accessibility Assessment, by a qualified Supplier Personnel, at any Site or End User's home address to determine the most appropriate items from the Products and Services Catalogue to meet their needs.
EUC-ADS-05	The Supplier shall, co-operate with the Customer and Third-Party Suppliers when arranging and conducting the Accessibility Assessment. The Supplier shall, ensure that proposed solutions are coordinated with other assessments.
EUC-ADS-06	The Supplier shall, as part of fulfilment of the request for an Accessibility Assessment, produce a report recommending a suitable Solution for the User.
EUC-ADS-07	The Supplier shall, on request from the Customer, conduct an accessibility training of recommended Solutions to End Users at any Site or, where required, an End User's home address.
EUC-ADS-08	The Supplier shall, conduct accessibility training and configurations, within five Working Days of the request being made, unless the accessibility training relates to a product that is not listed within the Products and Services Catalogue, in which case a separate timescale may be agreed with the Customer.
EUC-ADS-09	The Supplier shall, provide exception reports, as agreed with the Customer, on all requests and Incidents for Accessibility Solution Services that have not been delivered within the timescales of any relevant Service Levels and Call Off Contract KPIs.

6.9 Security

This Service defines the Post Office Security Requirements in relation to the EUC Services.

POL00337657

6.9.1 Security

The Supplier is required to delivery Security services pursuant to **RM3804-Alternative-and-additional-tc-v4, Schedule E Security Requirements**, and in addition the requirements defined below:

Req ID	Requirement Description
EUC-SEC-01	The Supplier shall, implement and maintain the controls to the levels laid out in the Customer's Security Policy & Standards.
EUC-SEC-02	The Supplier shall, in agreement with the Customer, detail, implement and maintain their Cyber Security model and describe how it adheres to the Customer Security Policy, Standards & Governance.
EUC-SEC-03	The Supplier shall, in agreement with the Customer, detail, implement and maintain the specific Cyber Security controls to be used for End User Computing (EUC) at the enterprise, network, platform, application and data level to protect services and data.
EUC-SEC-04	The Supplier shall, assure the Customer's data owners that they provide full disclosure (aka 'transparency') regarding security practices and procedures as stated in their SLAs, Customer's Security Policy & Standards and Cyber Security controls
EUC-SEC-05	The Supplier shall, in agreement with the Customer, detail, implement and manage how encryption is managed across all offerings.
EUC-SEC-06	The Supplier shall, in agreement with the Customer, detail, implement and manage the segregation of data between Customer's and environments.
EUC-SEC-07	The Supplier shall, in agreement with the Customer, detail, implement and manage the practices used for data cleansing.
EUC-SEC-08	The Supplier shall, in agreement with the Customer, detail, implement and manage the controls in place to access the Customer's cloud resources, providing services and processing data.
EUC-SEC-09	The Supplier shall, in agreement with the Customer, detail, implement and manage the controls that are in place to prevent loss of service or data availability.
EUC-SEC-10	The Supplier shall, in agreement with the Customer, detail, implement and manage the Cyber security standard operating procedures documented in place for the delivery of the service.
EUC-SEC-11	The Supplier shall, in agreement with the Customer, detail, implement and manage a robust solution for protection against malware and malicious software.
EUC-SEC-12	The Supplier shall, in agreement with the Customer: (a) conduct Security Tests (IT Health Check Security Test), at least annually, across the scope of the contract by an independent Third Party and additionally after any change or amendment to the service that falls below the agreed standards and terms, as set out in the Customer's Security and IT policies and standards; and (b) from the Security Tests detail the findings and remediation reports providing the Customer with a remediation plan to resolve any findings.
EUC-SEC-13	The Supplier shall, in agreement with the Customer, document and manage a vulnerability management process which will address: (a) how and when testing takes place; and (b) how and when vulnerabilities are reported, remediated and signed off.

POL00337657

EUC-SEC-14	The Supplier shall, in agreement with the Customer, provide details of named individuals (key personnel) who will be assigned duties detailing: (a) experience; (b) qualifications; and (c) security vetting clearance.
EUC-SEC-15	The Supplier shall, if they are not compliant with PCI SSC standards for any reason, will inform the Customer in writing of the non-compliance or likely non-compliance.
EUC-SEC-16	The Supplier shall take all steps, in accordance with Good Industry Practice, to prevent the introduction, creation or propagation of any disruptive elements (including any virus, worms and/or trojans, spyware or other malware) into systems, data, software or Customer Confidential Information (held in electronic form) owned by or under the control of or used by the Customer.
EUC-SEC-17	The Supplier shall deploy and maintain, throughout the Term, an ISO27001 Information Security Management System (ISMS) certified by an accredited certifying body and integrated with the cross-supply chain. The ISMS scope shall include technology; people; process; and locations used for the delivery of services to the Customer and the ISMS scope agreed & shared with the Customer.
EUC-SEC-18	The Supplier shall, in agreement with the Customer, document and manage the solution for logging of critical security and service events, provided for systems audit, security audit and incident management purposes. The Supplier shall, agree with the Customer the period for which logged events are retained.
EUC-SEC-19	The Supplier shall, ensure that all security events must be configured in agreement with the Customer within the native security event management system.
EUC-SEC-20	The Supplier shall, provide access to security related logs against all assets/services where the Customer Intellectual Property is processed and/or stored, in the form of ingestible logs into a SIEM tooling.
EUC-SEC-21	The Supplier shall, in agreement with the Customer, ensure it has secure procedures to mitigate threats from social engineering within the Supplier's organisation including any sub-contractors.
EUC-SEC-22	The Supplier shall, detail, implement and manage a process on how security incident and event management reporting data will be made available to the Customer for the purposes of supporting Customer-led governance, compliance and incident management activities.
EUC-SEC-23	The Supplier shall, in the event of a data breach or major Cyber Security incident, participate in Customer-led incident management activities and make available appropriate staff and other resources to allow a full investigation of the incident.
EUC-SEC-24	The Supplier shall, regularly audit and review its information security controls, processes, policies and procedures to ensure their continued effectiveness and determine whether adjustments are reasonably required in light of new circumstances including, without limitation, changes in technology, changes in information systems and threats or hazards to Data or to delivery of the Services.
EUC-SEC-25	The Supplier shall, in agreement with the Customer, have a process in place to assess the criticality of security updates, against the Customer's estate, and provide a deployment plan.
EUC-SEC-26	The Suppler shall, support e-discovery of data on an End User device at the instruction of the Customer's authorised personnel.

POL00337657

6.9.2 End User Computing (EUC) Build

This Service provides the configuration, testing, installation, commissioning, operation, monitoring, maintenance, tuning, modification and decommissioning of Post Office desktop standard operating environment ("SOE"), including laptops, desktops, Mobile Devices and Peripheral Devices

Req ID	Requirement Description
EUC-EUCB-01	The Supplier shall, ensure all the Customer's Data is protected, in accordance with its classification and criticality, against threats to confidentiality and integrity, as it transits any untrusted or uncontrolled networks which may include, but is not limited to: (a) the use of aggregating, channel-level, IPsec or TLS VPNs; and (b) per-Application or stream level.
EUC-EUCB-02	The Supplier shall, ensure the data stored on the device will be encrypted when the device is in its "rest" state. For always-on devices, like tablet devices, this is when the device is locked.
EUC-EUCB-03	The Supplier shall, ensure a user is only granted access to the device after successfully authenticating to the device.
EUC-EUCB-04	The Supplier shall, ensure any attempts by users to circumvent access controls by making modifications to the device, including "jailbreaking" or "rooting", the device shall be reported to the Customer.
EUC-EUCB-05	The Supplier shall, ensure a user is only able to access enterprise services after successfully authenticating to the service, via their device.
EUC-EUCB-06	The Supplier shall, provide access to enterprise services which is determined by authentication of the user and/or the device.
EUC-EUCB-07	The Supplier shall, ensure End Users, and where applicable devices, shall be granted access only after appropriate authentication and authorisation for such access has been verified. The level of access and any restrictions on access (e.g. controls on usage on the device) shall be determined based on the Customer's standards.
EUC-EUCB-08	The Supplier shall, ensure any unauthorised entity shall not be able to modify the boot process of a device, and any attempt to do so should be detected.
EUC-EUCB-09	The Supplier shall, implement application-level control to ensure that continued secure operation of the device is possible, even if an application or process is compromised.
EUC-EUCB-10	The Supplier shall, document how they manage the integrity of critical system files.
EUC-EUCB-11	The Supplier shall, ensure the Customer can define which applications are able to execute on the device, and these policies are robustly enforced on the device.
EUC-EUCB-12	The Supplier shall, ensure the device can detect, isolate and defeat malicious code which may impact the device.
EUC-EUCB-13	The Supplier shall, deploy anti-virus software on all systems commonly affected by malicious software, and ensure that the antivirus programme is capable of detecting and removing all known types of malicious software.

POL00337657

EUC-EUCB-14	The Supplier shall, ensure Security policies set by the Customer are robustly implemented across the platform. The Supplier will technically enforce a minimal set of security-critical policies on the device which cannot be overridden by the End User.
EUC-EUCB-15	The Supplier shall, ensure the device is able to constrain the set of ports (physical and logical) and services exposed to networks and devices.
EUC-EUCB-16	The Supplier shall, issue security updates and remotely validate the vulnerability level of your entire device estate.
EUC-EUCB-17	The Supplier shall, ensure the device reports security-critical events to their audit and monitoring service, and where required the Customer's SOC (Security Operation Centre). The user MUST be prevented from tampering with this reporting.
EUC-EUCB-18	The Supplier shall, maintain logs of all key events and where required by the Customer assist in identifying or investigating incidents, including but not limited to, breaches of access rights occurring in relation to the Customer's Data.
EUC-EUCB-19	The Supplier shall, keep such logs as specified by the Customer's Data Retention Policies and Processes.
EUC-EUCB-20	The Supplier shall, ensure they have an incident response plan and understand the impact of security incidents. This should be supported by appropriate functionality within the devices.
EUC-EUCB-21	The Supplier shall, within 24 hours, notify the Customer of any incident affecting cardholder, personal or business sensitive information. Information collected needs to follow chain of custody.

6.10 Project Services

Support the Post Office change activities via the Project Portfolio Management activities to identify, select, prioritise and evaluate projects in order to deliver the defined work order for any commercially agreed projects.

6.10.1 Project Change Management

Project services in the Post Office is in respect of changes that are large in scope and scale.

The Suppliers project services falls into two categories; the supplier carrying out entire projects on behalf of Post Office, and the supplier providing resource into Post Office managed projects.

The supplier in line with the requirement below will have a project engagement point to Post Office to which requests for new projects are submitted via a RTQ request and a PMO function in order to coordinate and control project activity.

When the supplier has been requested to deliver into a Post Office managed project, the supplier will provide work items, SME time or other inputs in line with the Post Office ways of working and governance.

Where projects are managed by the supplier on behalf of Post Office, the projects are to be governed and steered by Post Office. The supplier must manage the project in accordance with the Post Office project framework which includes a requirements phase, technology design, addressing security needs, and handover into service.

Req ID	Requirement Description

POL00337657

EUC-PCM-01	The Supplier shall, adhere to the Customer's Change Excellence Framework (CEF).
EUC-PCM-02	The Supplier shall, work within the Customer's Change Framework and where different from internal Supplier delivery methods, policies and processes the Customer's Change Framework will take precedence.
EUC-PCM-03	The Supplier shall, comply with the Customer's Quality Standards.
EUC-PCM-04	The Supplier shall, in agreement with the Customer establish a Project Portfolio Office to support the delivery and management of projects.
EUC-PCM-05	The Supplier shall, where requested by the Customer, update project, portfolio information and data via the Customer's project and portfolio tooling solution.
EUC-PCM-06	The Supplier shall, provide inputs to support the Customer in undertaking Project Portfolio Management activities to identify, select, prioritise and evaluate projects.
EUC-PCM-07	The Supplier shall, provide input and support to project requirements that apply across the IT Services and require cooperation and joint work between the Customer, other Supply Chain Members and Third-Party Vendors to come to a common solution.
EUC-PCM-08	The Supplier shall, ensure that all project requirements demonstrate economic viability, best practice and benefits for the Customer.
EUC-PCM-09	The Supplier shall, assist the Customer to initiate the Project Portfolio Management process for the Services in scope of the Agreement. This includes, but is not limited to: (a) collecting and consolidating project data as specified by the Customer (i.e. business drivers, business functions, benefits, costs, risks, status, project plans etc.); (b) identifying stakeholders, business drivers and priorities; (c) identifying the initial Project repository; (d) categorising, aligning and prioritising Projects; and (e) creating a Project Portfolio of all Customer Projects.
EUC-PCM-10	The Supplier shall, as part of each annual planning cycle (demand planning), provide information and data to assist the Customer with: (a) identifying upcoming Projects for the Services in scope; (b) identifying strategies, approaches, and Projects for future delivery of the Services; (c) identifying specific short-term steps and schedules for Projects or Changes expected to occur within the next twelve (12) months; (d) providing required data to update the Project inventory; and (e) constraints e.g. change freezes or business continuity activities.
EUC-PCM-11	The Supplier shall, deliver data and information to assist the Customer to prioritise projects and interdependencies between Projects.
EUC-PCM-12	The Supplier shall, provide all necessary data to assist the Customer to finalise and maintain the Project Portfolio contents, interrelationships and implementation priorities.
EUC-PCM-13	The Supplier shall, participate in the quarterly review of the Project Portfolio which includes but not limited to: (a) the presentation on, and discussion of, recommendations regarding Changes to the Project Portfolio; (b) identifying adjustments required based on the Suppliers participation in the monthly Project Portfolio reviews, focusing on Project Portfolio dashboard summary information and exception reporting items.

POL00337657

EUC-PCM-14	The Supplier shall, participate in the monthly Project Portfolio reviews and provide input as required, including but not limited to: (a) project information e.g. milestone, RAID, financials and progress update; (b) supporting the review of deliverables to understand the status and implications; and (c) preparing recommendations for the next quarterly Project Portfolio review meeting on any adjustments that should be made.
EUC-PCM-15	The Supplier shall, participate in ad-hoc Project Portfolio reviews, as requested by the Customer, which are typically invoked either by: (a) project performance findings during the monthly Project Portfolio review meetings that cannot wait for the next scheduled quarterly Project Portfolio review meeting; or (b) by the need to evaluate a new Project for addition to the existing Project Portfolio.
EUC-PCM-16	The Supplier shall, update its Project schedules and planning with the outcome of the Project Portfolio Management reviews.
EUC-PCM-17	The Supplier shall, deliver a Project Management Service employing a recognised Project Management methodology in accordance with Good Industry Practice.
EUC-PCM-18	The Supplier shall, ensure that the Project Management processes integrate with the Customer's other processes, e.g. Service Transition, Release and Deployment Management and Operational Change Management processes.
EUC-PCM-19	The Supplier shall, on receipt of a Project or Service Request, provide suitably skilled staff to support the Customer in the provision of Project Services.
EUC-PCM-20	The Supplier shall, for each Customer Project Deliverable, ensure they deliver the requirements and key success factors within agreed time, cost and quality parameters.
EUC-PCM-21	The Supplier shall, provide representation to input and update project board meetings or forums as agreed with the Customer.
EUC-PCM-22	The Supplier shall, utilise and share with the Customer its "best practice" in providing various Project Management services (depending on the project desired methodology e.g. Waterfall/Agile) with the intention of ensuring and improving the efficient operation and management.
EUC-PCM-23	The Supplier shall, where requested by the Customer perform a Post Implementation Review (PIR) and provide the Customer with a request to close report which outlines any lessons learned.
EUC-PCM-24	The Supplier shall, where requested by the Customer provide a project closure performance survey to enable project closure and stakeholders to feedback on the overall project delivery.
EUC-PCM-25	The Supplier shall, establish and maintain the Project, Programme and Portfolio Risk, Assumptions, Issues and Dependencies (RAID) and track and manage with the Customer to mitigate and resolve.
EUC-PCM-26	The Supplier shall, in agreement with the Customer, provide a finance forecast tracker for projects, programmes and portfolios which is reviewed in line with the finance timeline.
EUC-PCM-27	The Supplier shall, at the end of the project, participate in Post Project Reviews when requested by the Customer.

6.10.2 Operational Business Change (OBC)

POL00337657

The Post Office Operational Business Change Service (OBC) is the process used to support the delivery of both business and IT driven changes within the Post Office Branch network, for example the opening, closing, refurbishment, resizing or re-location of a Branch. IT is just one element of the Post Office OBC project activity.

The Post Office have a specific team that acts as the single point of contact for the coordination and management of the IT elements delivered by Post Office IT Suppliers and provides support and change activity across the Branch Infrastructure.

The purpose of the OBC process is to ensure that all Stakeholders roles, responsibilities and activities are defined and documented for each of the main OBC types.

The EUC provider is responsible for Counter Point of Sale devices and peripherals for branch opening installation, moves and closures/decommissioning which includes but is not limited to:

- Dynamic works risk assessment.
- Visual check on counters.
- Arranging delivery and install of Counter PoS components (including configuration health checks, Pin pads, Chain of Custody).
- Connecting cabling (including performing cabling diagnostic tests, basic data cabling and clipping to existing fabric /cable trays).
- Power-up and installation checks of PoS system and peripherals.
- Book the courier delivery of equipment /collection of packaging.
- Maintenance visits (including ad-hoc visits)
- Branch closure decommissioning and return of counter PoS devices and peripherals.

Appendix A: Ref Doc- 009 Post Office OBC Process Document

PCI Compliance - Chain of Custody

The Post Office use the Chain of Custody (CoC) for managing the deployment of Post Office Branch PIN Pad payment devices. The term “chain of custody” (CoC) refers to the order in which items of evidence have been electronically logged and/or documented during the handling and management of PIN Pads. Proving that a PIN Pad has been properly handled through an unbroken chain of custody is required for it to be considered as conforming to the Point to Point Encryption standard (P2PE). The chain of custody will show where the device was manufactured, key injected, shipped, stored, deployed, and finally disposed of, so that there is no question of its authenticity and that it will perform as promised, also ensuring that there has been no tampering or contamination.

All PIN Pads will need to have an established CoC before they can be linked to the Ingenico P2PE service. The Ingenico Terminal Management System (TMS) and asset tracking solution for inventory and CoC controls will be utilised by Post Office and as such would be the main point of control. The EUC Supplier is expected to maintain the evidence electronically within TMS as part of the services provided. Any doubt regarding the authenticity of information entered in TMS would necessitate the originating information from the service provider to be checked e.g. shipping details, inventory counts, etc. and corrections made.

Note: Interchangeable terms for PIN Pad = PIN Entry Device (PED) = Point of Interaction (POI)

POL00337657

Req ID	Requirement Description
EUC-OBC-01	The Supplier shall, establish a dedicated Operational Business Change (OBC) Project Management Office to support the Customer's OBC delivery team.
EUC-OBC-02	The Supplier shall, adhere to the Customer's tooling, standards, processes and ways of working.
EUC-OBC-03	The Supplier shall adhere to the Customer's timelines in delivery of the OBC Requests: (a) Branch Opening 10 working days; (b) Branch Closure (emergency) 24 hrs; (c) Branch Closure (normal) 5 working days; (d) Branch Relocations 10 working days; and (e) Next day delivery to Branch.
EUC-OBC-04	The Supplier shall, provide OBC Field Engineer Support to cover the full geographical spread of the Customer Branch estate including Northern Ireland, highland and island and other remote locations.
EUC-OBC-05	The Supplier shall, provide an agreed rate card for delivery of all the defined OBC request types.
EUC-OBC-06	The Supplier shall, provide a cost estimate to perform all the tasks associated with the OBC request that are identified outside of the rate card agreement and gain approval from the Customer, as applicable, prior to starting work.
EUC-OBC-07	The Supplier shall, forecast and coordinate resource allocation with the Customer for approved OBC Requests.
EUC-OBC-08	The Supplier shall, record, track, and manage all OBC Requests in coordination the Customer.
EUC-OBC-09	The Supplier shall, provide OBC Request status reports as appropriate and participate / attend the Customer's OBC planning meetings.
EUC-OBC-10	The Supplier shall, provide billing information requested by the Customer for rate card and non-rate card charges including expenses related to OBC Requests.
EUC-OBC-11	The Supplier shall, provide and perform post-implementation reviews of OBC Requests as request by the Customer.
EUC-OBC-12	The Supplier shall, integrate and support the Customer's escalation process.
EUC-OBC-13	The Supplier shall, provide the Customer with an estimated time of arrival for all Engineer Visits and inform of any changes to ETA's at a minimum one day in advance.
EUC-OBC-14	The Supplier shall, be accountable at all time without exception for the management and delivery of applicable PCI compliance activities associated with the OBC process.
EUC-OBC-15	The Supplier shall, ensure that all relevant documentation, including job sheets, is signed-off by the respective Branch representative.
EUC-OBC-16	The Supplier shall, be responsible for all data cabling activities, except where there is a Branch fit out and its more efficient for this to be undertaken by another Third-Party, and agreed with the Customer.

6.10.3 Service Design and Transition

Service Transition process ensures the orderly transition of a new or modified service into production, together with the necessary adaptations to the service management processes. This must incorporate the service design and operational requirements within the transition planning.

POL00337657

Req ID	Requirement Description
EUC-SDT-01	The Supplier shall, at all times adhere to the Customer's Service Design and Transition Management Policies and Processes in the delivery of their Services.
EUC-SDT-02	The Supplier shall, provide dedicated Service Design and Transition resources who are accountable for the delivery of change.
EUC-SDT-03	The Supplier shall, track and deliver all Service Design and Transition activities utilising the Customer's tooling solution.
EUC-SDT-04	The Supplier shall, follow the lifecycle stages for the Service Design and Transition as set out by the Customer and the move from one stage to the next will be subject to formal checks & acceptance.
EUC-SDT-05	The Supplier shall, in agreement with the Customer, produce a Service Design Package defining but not limited to the Support model, Operating Times, Service Levels, Transition activities, testing and early life support approach.
EUC-SDT-06	The Supplier shall, deliver the full end to end transition activities including the Customer's deliverable to ensure that the agreed Service Design Package is developed, built and operational in alignment with the Customer's standards.
EUC-SDT-07	The Supplier shall, work with the Customer to define the Service Design and Transition responsibilities and deliverables, objects, products, training and acceptance criteria.
EUC-SDT-08	The Supplier shall, in collaboration with the Customer and where appropriate the Third-Party Suppliers, develop Service Design and Transition plans that describe the tasks and activities to roll out a change in development, test and production environments.
EUC-SDT-09	The Supplier shall, in agreement with the Customer, develop and deliver an operational acceptance test prior to acceptance into service.
EUC-SDT-10	The Supplier shall, in agreement with the Customer, ensure an Acceptance into Service Certificate and formal meeting is conducted across all supporting parties prior to a change moving to production.
EUC-SDT-11	The Supplier shall, in agreement with the Customer, deliver Early Life Support (ELS) in a project delivery phase.
EUC-SDT-12	The Supplier shall, in agreement with the Customer, meet all ELS criteria as a condition of project closure.

6.10.4 Request to Quote (RTQ)

The RTQ process (often known in the IT industry as RFS or Work Order process) is used to capture changes which are carried out by Suppliers which are non-standard, chargeable and which need to be quoted for. RTQ tends to be a large in scope of work than that of a BAU Change and smaller than that of a project.

The RTQ process corresponds to the Post Office Project Management ServiceNow module.

Post Office have an RTQ team which manage the RTQ workflow which is initiated by users submitting the initiating requested into an online portal. The team progress RTQ work item approvals which consist of an initial CTO and Data Protection approval, followed by review board, and an internal approval process which includes CTO, security, finance, and commercial approvals followed by the supplier submission.

Service Levels: RTQ requests responses shall be bound by the corresponding Service Levels defined in the Service Levels Section 7. There are no predefined SLAs for RTQ fulfilment time, and in this respect the fulfilment time agreed during the initiation phase shall

POL00337657

be binding, meaning that the supplier is responsible for the labour cost of overruns, meaning RTQ delivery that runs past the agreed date of delivery.

Req ID	Requirement Description
EUC-RTQ-01	The Supplier shall, establish a Project Management function to support the Customer's requests for project, operational statements of work and governance of the service.
EUC-RTQ-02	The Supplier shall, adhere to the Customer's Request to Quote (RTQ) process.
EUC-RTQ-03	The Supplier shall, be responsible for the labour cost of overruns for any RTQ delivery that runs past the agreed date of delivery.
EUC-RTQ-04	The Supplier shall, archive all RTQs for up to 12 months.
EUC-RTQ-05	The Supplier shall, provide a representative to attend RTQ review meetings to assess and accept RTQ into the supplier process.
EUC-RTQ-06	The Supplier shall, develop and submit to the Customer a written RTQ response, including a timeline, milestones, resource utilisation and costs to complete the Request in accordance with the Customer's process.
EUC-RTQ-07	The Supplier shall, produce a completed RTQ within 10 working days of receiving the approved request, unless agreed prior to submission of the request with the Customer.
EUC-RTQ-08	The Supplier shall, ensure the RTQ response addresses all requirements of the RTQ with traceability of the RTQ owner's requirements to the proposed solution & costs.
EUC-RTQ-09	The Supplier shall, deliver the RTQ service using the Customer's IT Business Management (ITBM) tool.
EUC-RTQ-10	The Supplier shall, identify economies of scale and synergies across multiple RTQ's, where possible, and indicate these possible savings to the Customer.
EUC-RTQ-11	The Supplier shall, respond to challenges and questions to the Supplier's RTQ Response.
EUC-RTQ-12	The Supplier shall, cooperate with other Customer suppliers, where required, to respond to RTQs.
EUC-RTQ-13	The Supplier shall, deliver a function in support of the Customer's ideation needs for project opportunities for the delivery of Rough Order of Magnitude (ROM) reports.
EUC-RTQ-14	The Supplier shall, develop and submit to the Customer a written Ideation response, including ROM timeline, costs and outline solutions options.
EUC-RTQ-15	The Supplier shall, produce a completed Ideation response within 10 working days of receiving the approved request, unless agreed prior to submission of the request with the Customer.
EUC-RTQ-16	The Supplier shall, make available the appropriate skilled resources to work with the Customer in the delivery of Ideation requests.

6.11 Monitoring and Reporting

Regular check and monitor the uptime of infrastructure components such as servers and apps and notifying the support services of problems before they impact the business.

6.11.1 Availability Management

This service ensures all services provided to Post Office are available in line with the agreed availability service levels. The availability service levels defined in the Service Levels

POL00337657

section need to be proactively measured for the levels of availability using agreed mechanisms, measures and metrics.

To ensure that the business needs of service are meet all infrastructure is measured using availability polling, for example through monitoring systems, in order to directly arrive at an availability figure.

Availability management should be seen as proactive process by managing failure risks and single points of failure in the infrastructure and utilising service dashboards and reporting (where agreed and applicable).

Req ID	Requirement Description
EUC-AVM-01	The Supplier shall, work with the Customer in defining the delivery of the Availability Management process and agree ways of working.
EUC-AVM-02	The Supplier shall, have the appropriate monitoring and measurement in place to support the Customer's service levels.
EUC-AVM-03	The Supplier shall, establish and develop a maintenance strategy in agreement with the Customer to ensure availability levels.
EUC-AVM-04	The Supplier shall, as agreed with the Customer, produce and manage a non-compliance report against the Customer's Availability Management processes, ways of working and Service Levels.
EUC-AVM-05	The Supplier shall, make recommendations to improve the resilience and Availability of in-scope IT Services and Business Services to the Customer.
EUC-AVM-06	The Supplier shall, assist the Customer in working with Third Party Suppliers and internal support groups as appropriate to ensure Availability targets can be met for new and existing Services.
EUC-AVM-07	The Supplier shall, proactively monitor Availability levels and trends to identify potential threats to Availability at the earliest opportunity.
EUC-AVM-08	The Supplier shall, utilise automatic reporting agents, where applicable and in agreement with the Customer, to measure availability trends and targets.
EUC-AVM-09	The Supplier shall, in agreement with the Customer, be accountable for defining and setting of automated alerts to trigger when Availability thresholds are breached.
EUC-AVM-10	The Supplier shall, organise and facilitate a monthly management meeting to report on but not limited to current resource utilisation, trends, forecasts, and exceptions in an agreed format.

6.11.2 Capacity Management

With the delivery of cloud services and their respective applications there is a need to ensure that the service meet the agreed capacity requirements through understanding both seasonal and long-range changes in the demand of the Post Office business.

The service will use the capacity thresholds, the metrics and mechanics of measuring capacity utilising tooling in order to assist with measurement and management of capacity, for example monitoring systems which detect disk, Central Processor Unit (CPU) and memory capacity utilisation levels in computers.

Where capacity issues are identified the supplier shall work in a timely way and via the appropriate forums, for example Problem tickets or SIP items to mitigate.

POL00337657

Capacity reporting will be carried out in conjunction with capacity plans which provide the current capacity levels, forecasts in demand and details of future initiatives to alter capacity of supply.

The supplier will work with the business in order to understand expected change in the future levels of business demand from the Post Office branch business, forecasting demand using tending techniques, remediating capacity issues prior to operational impact.

Req ID	Requirement Description
EUC-CM-01	The Supplier shall, work with the Customer in defining the delivery of the Capacity Management process and agree ways of working.
EUC-CM-02	The Supplier shall, undertake forward capacity management planning which includes identification of exceptions, review of reports and trends in relation to the Services.
EUC-CM-03	The Supplier shall, deploy proactive Capacity Management monitoring and reporting in relation to the Services, which includes but not limited to:- (a) prevent Incidents and Problems related to resource utilisation from occurring; (b) trend current system, resource and estimate future utilisation; (c) model seasonal patterns of business activity and BAU growth; and (d) reviewing under and over utilisation and pro-actively undertake remediation actions.
EUC-CM-04	The Supplier shall, develop, monitor, track and complete remediation action plans to address any capacity deficiency or surplus in respect of their Services.
EUC-CM-05	The Supplier shall, align the capacity management process to the Customer's business and IT plans. This includes performing an analysis in support of business planning, capacity and utilisation studies for its Services.
EUC-CM-06	The Supplier shall, analyse the demand forecast and submit recommendations for capacity changes for its Services.
EUC-CM-07	The Supplier shall, update the Customer knowledge base of capacity constraints and impact of future demand.
EUC-CM-08	The Supplier shall, where possible, estimate and report the resource and utilisation effects of cross functional changes that impact their Services.
EUC-CM-09	The Supplier shall, organise and facilitate a monthly management meeting to report on, but not limited to, current resource utilisation, trends, forecasts, and exceptions in an agreed format.
EUC-CM-10	The Supplier shall, produce and maintain Capacity Plans for the EUC Services which include, but is not limited to: (a) fluctuations in business as usual capacity demand; (b) planned business change; (c) patterns of Business Activity; (d) revised or new Service Levels; (e) revised or new EUC Services; (f) ITSCM; (g) transition requirements; and (h) the impact of emerging technologies within the Service pipeline.
EUC-CM-11	The Supplier shall, optimise resource utilisation in a cost-effective manner.

POL00337657

6.11.3 Event Management

This service manages System /Solution Events throughout their Lifecycle. Supplier Event Management is delivered in conjunction with Post Office Operational Management to ensure the risk and integrity of IT systems.

Req ID	Requirement Description
EUC-EM-01	The Supplier shall, work with the Customer in defining the delivery of the Event Management process and agree ways of working.
EUC-EM-02	The Supplier shall, where requested integrate events and alerts with the Customer's ITSM product and other platforms (e.g. AWS Data Platform) for the purpose of event correlation and aggregation when requested by the Customer.
EUC-EM-03	The Supplier shall, relate EUC events to IT Systems, Infrastructure and Application services so that a Priority assessment can be made by all parties.
EUC-EM-04	The Supplier shall, implement and maintain event monitoring mechanisms and Business Rules, including the activities necessary to set up and maintain the mechanisms for generating meaningful events and effective rules for their filtering and correlating.
EUC-EM-05	The Supplier shall, establish and maintain a proactive and automated event management process to ensure all Services are monitored and that agreed events are identified, promptly actioned, recorded and reported.
EUC-EM-06	The Supplier shall, set and report on thresholds agreed with and approved by the Customer, which may be subject to change during the Term.
EUC-EM-07	The Supplier shall, participate in joint coordination meetings organised by the Customer to determine response selection for cross-functional Events.
EUC-EM-08	The Supplier shall, be responsible for the end-to-end event response and communication between all in-scope parties; that is, being responsible from the time the event was originally logged to the point at which it is deemed to be resolved.
EUC-EM-09	The Supplier shall, be responsible for coordinating triage activities and invoking event escalations, as required.
EUC-EM-10	The Supplier shall, provide and manage tools and processes to correlate and action events based upon the various alerts and their criticality.
EUC-EM-11	The Supplier shall, provide proactive and reactive monitoring (including trending analysis) and management in order to enhance the stability and function of Customer Business Services and IT Services.
EUC-EM-12	The Supplier shall, correlate events to facilitate Problem Management and Root Cause Analysis (RCA) and make event-related trend analysis available.

6.11.4 IT Operations Centre

The EUC Supplier function responsible for Monitoring and Control of the Post Office IT Services and IT Infrastructure delivered by the supplier.

Req ID	Requirement Description
EUC-ITOC-01	The Supplier shall, adhere to, the Customer's Service Management Policies and Processes as applicable to the scope of the Services.

POL00337657

EUC-ITOC-02	The Supplier shall, provide monitoring, reporting, maintenance & control for the delivery of the services. This shall also include: (a) ensuring SLA & KPI targets are met; (b) identification of potential risk and interruptions to service; (c) minimising service interruptions; (d) the restoration of service; and (e) identifying opportunities to improve services, reduce cost, support satisfaction for end users.
EUC-ITOC-03	The Supplier shall, establish and manage controls to ensure that the service is auditable and meets the Regulatory and Policy requirements of the Customer.
EUC-ITOC-04	The Supplier shall, establish, maintain and enhance IT Operations Centre Processes, Governance and Tools that support the Supplier's end to end responsibility and enable it to provide consistent management, coordination and communication of the delivery of the IT Operations Centre services across the supply chain.
EUC-ITOC-05	The Supplier shall, maintain comprehensive documents and records in connection with the provision of the IT Operations Centre services and shall provide to the Customer such supporting documentation as the Customer may reasonably require in order to verify the Supplier's compliance with all applicable policies, processes and service obligations.
EUC-ITOC-06	The Supplier shall, in agreement with the Customer, promote process efficiency and data quality consistency to ensure that the IT Operations Centre is designed to capture data once, minimising the need for manual data capture and input. All data will, wherever possible, be validated by the ITSM Toolset on input.
EUC-ITOC-07	The Supplier shall, assist the Customer in the identification of automation opportunities, development of tools/scripts and process enhancements (including assisting with integrations to other third-party toolsets where required), to proactively perform and automate the service management processes.
EUC-ITOC-08	The Supplier shall, work collaboratively with the Customer IT Service Desk and Branch Support centre.
EUC-ITOC-09	The Supplier shall, provide a Single Point of Contact for the Customer's Service Desks to engage/escalate issues.

6.11.5 Monitoring and Reporting

The Suppliers observance of a Configuration Item, IT Service or Process to detect Events (or lack of) and to ensure that the current status is known and made available to the Post Office.

Req ID	Requirement Description
EUC-MR-01	The Supplier shall, provide monitoring and reporting to effectively identify potential Incidents, Problems and performance improvements to ensure optimisation of the Service.
EUC-MR-02	The Supplier shall, analyse monitoring results to identify areas of the overall configuration that could be tuned or optimised, to better utilise the Service, system and component resources or improve the performance of that particular Service.
EUC-MR-03	The Supplier shall, capture operations data for the Services in accordance with the data specifications in agreement with the Customer.

POL00337657

EUC-MR-04	The Supplier shall, in agreement with the Customer, provide no more than monthly, a report detailing the performance of the Services against Service Levels, KPIs, making recommendations when identified.
EUC-MR-05	The Supplier shall, work collaboratively with the Customer to agree how Monitoring & Reporting is implemented for new CI's or Services.
EUC-MR-06	The Supplier shall, where requested by the Customer, integrate monitoring agents into all in scope technologies including: (a) End User devices; (b) Servers; and (c) Network components.

6.11.6 Demand Management

The Support of the Post Office to understand, anticipate, and influence our user/business demand for services. This means that demand for services can grow or shrink with the business cycle and the allocation of resource to meet these changes.

Req ID	Requirement Description
EUC-DM-01	The Supplier shall, nominate a dedicated on-site resource who shall act as the primary technical interface for Architecture and Demand Management for the Supplier.
EUC-DM-02	The Supplier shall, provide Demand Management for the EUC Services, including but not limited to: (a) developing EUC Service demand models and demand forecasts based on Patterns of Business Activity provided by the Customer; (b) make recommendations to reduce demands on EUC Services; (c) make recommendations on how Capacity Plans shall be affected by demand projections including the steps needed to meet demand projections; (d) make recommendations to the Customer for improvements of the mechanisms to control and meet current and forecast demand for EUC Services.
EUC-DM-03	The Supplier shall, provide on a monthly basis, the predicted consumption of the Services based on a framework that is jointly developed by the Customer, the Supplier and Third-Party suppliers.
EUC-DM-04	The Supplier shall, report to the Customer, in a timely manner, the inability to satisfy demand and provide service improvement plans to rectify the situation.
EUC-DM-05	The Supplier shall, translate and report on patterns of Business Demand from EUC Services.
EUC-DM-06	The Supplier shall, with approval from the Customer, implement a continuous improvement process for demand forecasting, through the acquisition of knowledge and data, to provide greater accuracy on predicted vs actual.

POL00337657

7. SERVICE LEVELS AND KEY PERFORMANCE INDICATORS

This section provides the Post Office business driven expectations of service levels. Service Levels Agreements (SLA) and Key Performance Indicators (KPI) are broken down and aligned to specific applications, services or the process of service delivery as opposed to using catch all Service Levels for the entire scope of supplier service. The SLAs & KPIs have been defined to meet the following drivers:

a. Alignment to specific business units (Branch vs Colleague),
b. Alignment to services used for specific functional reasons and
c. Alignment to the required criticality level of each service.

The Supplier will be responsible for performance against SLAs & KPIs in respect of the scope of responsibility that sits with its own operations and its subcontractor operations. The Supplier will not be responsible for performance during the time when a work item is assigned to Post Office operations or parties with which Post Office directly contracts.

Where possible the service metrics will be recorded within the Post Office ServiceNow platform. This will enable real time tracking for both parties and utilising the advanced performance analytics within ServiceNow management of demand constraints and trends.

The Supplier Service Management team will be the accountable team for ensuring that the delivery of the services is meeting or exceeding the contracted targets. Where a target is at risk or has been missed the supplier Service representative will liaise with the appropriate Customer representative to resolve, plan and deliver a remediation plan.

The Supplier is required to deliver Service Level Management services pursuant to **RM3804-Call-Off-tc-v6, Call off Schedule 3: Service Levels, Service Credits and Performance Monitoring.**

POL00337657

7.1 Service Level Agreements

This section sets out the Service Levels which the Supplier is required to achieve when providing the Services.

SLA Name	Service	Service Levels	Description	Formula	Service Level Target	Service Level Threshold	Service Credit for each Service Period	Service Hours	Reporting Period
EUC-IN-INC-01	Incident Management	P1 Major Incident resolution	A failure or outage that (i) affects the Customer IT infrastructure resulting in a loss of ability to trade, and/or deal with customers, and/or settle or report to regulators, and/or satisfy any regulatory obligation, and/or (ii) results in potential financial loss to Customer and/or damage to the reputation of Customer, and/or (iii) a significant impact to business operation (iv) a security breach/potential breach or data loss	C= (A/B)*100 A. The number of EUC-IN-INC-01 Incidents resolved within the specified timeframe for the Reporting Period. B. The total number of EUC-IN-INC-01 Incidents resolved within the Reporting Period. C. The percentage of EUC-IN-INC-01 Incidents Resolved within the specified Reporting Period.	0 breaches of the 4 Hours resolution time.	1 >=2	1.0% 2.0%	24x7	Monthly
EUC-IN-INC-02	Incident Management	P2 Significant Incident resolution	An Incident that is not a Major Incident, but one which is: (i) a degradation, failure or outage which has a serious internal impact that is likely to lead to delay or interruption to important, time critical working processes for a group and/or (ii) a failure or outage affecting multiple Users	C= (A/B)*100 A. The number of EUC-IN-INC-02 Incidents resolved within the specified timeframe for the Reporting Period. B. The total number of EUC-IN-INC-02 Incidents resolved within the Reporting Period. C. The percentage of EUC-IN-INC-02 Incidents Resolved	0 breaches of the 8 Hours resolution time	1 >=2	1.0% 2.0%	24x7	Monthly

POL00337657

			with no effective workaround.	within the specified Reporting Period.					
EUC-IN-INC-03	Incident Management	Priority 3 Standard Incident resolution	An Incident that is not a Major Incident or a Significant Incident which requires a standard response and recovery and is not covered by the Branch resolution 1 to 3 or Colleague Resolution 1 to 3	C= (A/B)*100 A. The number of EUC-IN-INC-03 Incidents resolved within the specified timeframe for the Reporting Period. B. The total number of EUC-IN-INC-03 Incidents resolved within during the Reporting Period. C. The percentage of EUC-IN-INC-03 Incidents Resolved within the specified Reporting Period.	98% within 12 Hours Service Hours	<98% <95%	0.5% 1.0%	Extended Support Hours 08:00 - 20:00 Monday - Friday 08:00 - 16:00 Saturday – Sunday	Monthly
EUC-IN-INC-04	Incident Management	Priority 4 Incident resolution	Any Incident that is not a Major Incident, a Critical Incident, or a Standard Incident	C= (A/B)*100 A. The number of SEUC-IN-INC-04 Incidents resolved within the specified timeframe for the Reporting Period. B. The total number of EUC-IN-INC-04 Incidents resolved within during the Reporting Period. C. The percentage of EUC-IN-INC-04 Incidents Resolved within the specified timeframe during the Reporting Period.	98% within 24 Service Hours	<98% <95%	0.5% 1.0%	Extended Support Hours 08:00 - 20:00 Monday - Friday 08:00 - 16:00 Saturday – Sunday	Monthly

POL00337657

EUC-BR-ENG-01	Engineering - Branch	Branch P3 standard incident Resolution level 1	A failure or outage that results in a complete failure of an individual Branch to trade and/or deal with Customers, or multiple counter branch with 75% reduction in availability	C= (A/B)*100 A. The number of EUC-BR-ENG-01 Incidents resolved within the specified timeframe for the Reporting Period. B. The total number of EUC-BR-ENG-01 Incidents resolved within the Reporting Period. C. The percentage of EUC-BR-ENG-01 Incidents Resolved within the specified timeframe during the Reporting Period.	95% within: 4 Service Hours for City & Town Branch's 5 Service Hours for Urban Branch's 6 Service Hours for Rural Branch's 12 Service Hours for Remote Branches	<95% <90%	3.0% 5.0%	Extended Support Hours 08:00 - 20:00 Monday - Friday 08:00 - 16:00 Saturday – Sunday	Monthly
EUC-BR-ENG-02	Engineering - Branch	Branch P3 standard incident Resolution level 2	Branch IT fault with reduced counter functionality and/or solution available through workarounds for single counter branch. Branches with up to 75% reduction in availability.	C= (A/B)*100 A. The number of EUC-BR-ENG-02 Incidents resolved within the specified timeframe for the Reporting Period. B. The total number of EUC-BR-ENG-02 Incidents resolved within during the Reporting Period. C. The percentage of EUC-BR-ENG-02 Incidents Resolved within the specified timeframe during the Reporting Period.	95% within: 24 Hours for City & Town, Urban and Rural Branches 36 Hours for Remote Branches	<95% <90%	1.0% 2.0%	Extended Support Hours 08:00 - 20:00 Monday - Friday 08:00 - 16:00 Saturday – Sunday	Monthly
EUC-BR-ENG-03	Engineering - Branch	Branch P3 standard incident Resolution level 3	Branch Requests or non-urgent call, spares management, postal service	C= (A/B)*100 A. The number of EUC-BR-ENG-03 Incidents resolved within the specified timeframe for the Reporting Period. B. The total number of EUC-BR-ENG-03 Incidents resolved within during the Reporting Period. C. The percentage of EUC-	95% within: 48 Hours for: City & Town, Urban and Rural Branches 72 Hours for: Remote Branches	<95% <90%	0.5% 1.0%	Extended Support Hours 08:00 - 20:00 Monday - Friday 08:00 - 16:00 Saturda	Monthly

POL00337657

				BR-ENG-03 Incidents Resolved within the specified timeframe during the Reporting Period.				y – Sunday	
EUC-BR-ENG-05	Engineering - Branch	Fixed First Time Branch Engineering	Incident signed-off by end customer at first visit	C= (A/B)*100 A. The number of incidents allocated to the supplier for a field engineer visit which the customer approves the completion of the work on the first visit within the reporting period B. The total number of Incidents requiring a field engineer visit allocated to the supplier within the Reporting Period. C. The percentage of Incidents resolved by field engineer at first visit.	95% of incident resolved on first visit within the service period	<95% <90%	1.0% 2.0%	Extended Support Hours 08:00 - 20:00 Monday - Friday 08:00 - 16:00 Saturday – Sunday	Monthly
EUC-CO-ENG-01	Engineering - Colleague	Colleague P3 standard incident Resolution level 1	A failure or outage of an end user device, software, application or EUC end user services that is linked to a VIP.	C= (A/B)*100 A. The number of EUC-CO-ENG-01 Incidents resolved within the specified timeframe for the Reporting Period. B. The total number of EUC-CO-ENG-01 Incidents resolved within the Reporting Period. C. The percentage of EUC-CO-ENG-01 Incidents Resolved within the specified timeframe during the Reporting Period.	98% within 4 Service Hours	<98% <95%	1.0% 2.0%	Extended Support Hours 08:00 - 20:00 Monday - Friday 08:00 - 16:00 Saturday – Sunday	Monthly

POL00337657

EUC-CO-ENG-02	Engineering - Colleague	Colleague P3 standard incident Resolution level 2	A failure or outage of an end user device, software, application or EUC end user services that is linked to a business critical user.	C= (A/B)*100 A. The number of EUC-CO-ENG-02 Incidents resolved within the specified timeframe for the Reporting Period. B. The total number of EUC-CO-ENG-02 Incidents resolved within the Reporting Period. C. The percentage of EUC-CO-ENG-02 Incidents Resolved within the specified timeframe during the Reporting Period.	98% within 8 Service Hours	<98% <95%	1.0% 2.0%	Extended Support Hours 08:00 - 20:00 Monday - Friday 08:00 - 16:00 Saturday – Sunday	Monthly
EUC-CO-ENG-03	Engineering - Colleague	Colleague P3 standard incident Resolution level 3	An Incident which requires a standard response and recovery.	C= (A/B)*100 A. The number of EUC-CO-ENG-03 Incidents resolved within the specified timeframe for the Reporting Period. B. The total number of EUC-CO-ENG-03 Incidents resolved within during the Reporting Period. C. The percentage of EUC-CO-ENG-03 Incidents Resolved within the specified timeframe during the Reporting Period.	98% within 12 Service Hours	<98% <95%	0.5% 1.0%	Extended Support Hours 08:00 - 20:00 Monday - Friday 08:00 - 16:00 Saturday – Sunday	Monthly
EUC-INF-SS-02	Infrastructure	Shared Service Technology	The individual resilient Wintel server Availability (Production & DR Environments)	The individual resilient Wintel server availability will operate at a level of Availability for 99.9% on a 24 x 7 basis	99.9% availability for the service period	<99.9% <99%	1.0% 2.0%	24 x 7	Monthly
EUC-INF-SS-03	Infrastructure	Shared Service Technology	The availability of production databases.	Individual production databases will be available for 99.9% on a 24 x 7 basis	99.9% availability for the service period	<99.9% <99%	1.0% 2.0%	24 x 7	Monthly

POL00337657

EUC-INF-SS-04	Infrastructure	Shared Service Technology	The availability of Directory Services	Individual Directory Services will be available for 99.9% on a 24 x 7 basis	99.9% availability for the service period	<99.9% <99%	1.0% 2.0%	24 x 7	Monthly
EUC-SEC-PAC-01	Security	Emergency Patching	Emergency security patches deployed to End User devices within 2 Working Days of notification to Supplier of such by Customer' information security team where patching is possible using an automated toolset	C= (A/B)*100 A. The number of End User devices with a successful patched within 2 working days and 5 working days B. The total number of End User devices that require the security patch C. The percentage of End User devices successfully patched within the specified timeframe during the Service Period.	95% within 2 Working Days 99.5% within 5 Working Days	<95% <99.5%	0.5% 1.0%	Extended Support Hours 08:00 - 20:00 Monday - Friday 08:00 - 16:00 Saturday – Sunday	Monthly
EUC-SEC-PAC-02	Security	Patching	Security patches deployed to Customers Managed End User Devices within 20 Working Days of security updates being released	C= (A/B)*100 A. The number of End User devices with a successful patched within 20 working days B. The total number of End User devices that require the security patch C. The percentage of End User devices successfully patched within the specified timeframe during the Service Period.	95% within 20 Working Days	<95% <90%	0.5% 1.0%	Extended Support Hours 08:00 - 20:00 Monday - Friday 08:00 - 16:00 Saturday – Sunday	Monthly
EUC-SEC-PAC-03	Security	Infrastructure Emergency Patching	Emergency security patches deployed to Wintel servers within 2 Working Days of security updates being released	C= (A/B)*100 A. The number of Wintel servers with a successful patched within 2 working days B. The total number of Wintel servers that require the security patch	95% within 2 Working Days	<95% <90%	0.5% 1.0%	24x7	Monthly

POL00337657

				C. The percentage of Wintel servers successfully patched within the specified timeframe during the Service Period.					
EUC-SEC-PAC-04	Security	Infrastructure Patching	Security update deployed to Wintel servers within 20 Working Days of security patches being released	C= (A/B)*100 A. The number of Wintel servers with a successful patched within 20 working days B. The total number of Wintel servers that require the security patch C. The percentage of Wintel servers successfully patched within the specified timeframe during the Service Period.	99.9% within 20 Working Days	<99.9% <99%	0.5% 1.0%	24x7	Monthly
EUC-OPS-REQ-01	Operations	Service Request Fulfilment	Percentage of Service Catalogue requests which are fulfilled on receipt of the customer within the required timescale in accordance with the Service Catalogue.	C= (A/B)*100 A. The number of service catalogue requests for which the Supplier is responsible which are receipted by the end user successfully and within the stated timeframe for that specific request as defined in the Service Catalogue for the Service Period. B. The total number of raised service catalogue requests that the Supplier is responsible for implementing during that Service Period. The percentage of service requests for which the Supplier is responsible, which are implemented successfully and within the stated time frame for that specific request as defined within the relevant	95% of request delivered to the specified timescale	<95% <90%	1.0% 2.0%	Extended Support Hours 08:00 - 20:00 Monday - Friday 08:00 - 16:00 Saturday – Sunday	Monthly

POL00337657

				Service Catalogue during the Service Period.					

Table 16: *EUC Service Level Agreements*

POL00337657

7.2 Key Performance Indicators

This section sets out the Key Performance Indicators which the Supplier is required to measure and report against for the Services.

KPI Name	Service	Key Performance Indicator	Description	Formula	Key Performance indicator Target	KPI Threshold	Service Credit for each Service Period not (appliable for KPI)	Service Hours	Reporting Period
EUC-CO-ENG-04	Engineering - Colleague	Fixed First Time Colleague	Incident signed-off by end customer at first contact of supplier support services	C= (A/B)*100 A. The total number of Incidents approved by the Colleague End User as Resolved on the first contact to action the work request. B. The total number of requests for Colleague End Users allocated to the supplier for resolution within a specified timeframe within the Service Period. C. The percentage of Colleague End User Incidents Resolved on first contact.	95% resolved on first contact by supplier engineering service teams	<98% <95%	1.0% 2.0%	Extended Support Hours 08:00 - 20:00 Monday - Friday 08:00 - 16:00 Saturday – Sunday	Monthly
EUC-CO-ENG-05	Engineering - Colleague	Colleague Customer Satisfaction net promoter score	Colleague End users response rating when surveyed after closure of a incident or request ticket that rated their experience between: 10-8 Excellent to very good 7-5 Good to satisfactory 4-1 disappointing to poor	The Net Promoter Score is the % of responses during the reporting period that when achieved a score between 10-8 (promoter) subtracted by the percentage that achieve a score between 4-1 (detractors)	NPS <0 for the reporting period	<30 <0	1.0% 2.0%	Monthly	Monthly

POL00337657

EUC-ENG-PUN-01	Engineering	Punctuality of field engineering	The punctuality of a Field Engineer arriving at their allocated destination within 15min of the allocated time slot in the schedule workorder and no later than the allocated time slot	C= (A/B)*100 A. The number of requests allocated to the supplier for a field engineer arriving at site and which are put in progress no earlier that 15 minutes of the ETA and no later than the defined timeslot. B. The total number of requests for a field engineer allocated to the supplier within the Service Period. C. The percentage of field engineer visits arriving and placing the workorder in progress within 15 min to the end time of the allotted slot to the	95% of engineers starting work within the defined timescale	<95% <90%	1.0% 2.0%	Extended Support Hours 08:00 - 20:00 Monday - Friday 08:00 - 16:00 Saturday – Sunday	Monthly
EUC-PRO-RTQ-01	Project	Request to quote	Percentage of Change Requests to the Supplier by the Customer that have a quote completed and returned to the Customer that are capable of being accepted by the Customer, within the allotted key performance indicator for the size/category of change. Minor: 5 Working Days Significant: 10 Working Days Major: 20 Working Days	C= (A/B)*100 A. The number of Change Requests for a change by size category that are completed to their respective category Call Off Contract KPI. B. The total number of Change Requests by size category that were requested of the Supplier by their respective size category. C. The percentage of Change Requests by size category that are completed to their respective size category Call Off Contract KPI.	97% of request delivered to the specified timescale	<97% <90%	1.0% 2.0%	Business Hours	Monthly

POL00337657

EUC-PRO-OBC-01	Project	Operational Business Change	The Supplier shall adhere to the Customer's lead times in delivery of the OBC Requests 12 working days to the commissioning date: Counter Commissioning Counter Commissioning (no on-site support) 10 working days to the Decommissioning date: Counter Decommissioning Counter Decommissioning (no on-site support) 30 working days: Branch Commissioning 5 working days to closure date: Branch Decommissioning 25 working days to the closure date Branch Relocation 12 working days to the closure date Branch Referb 8 working days to the closure date Branch Referb (no on-site support	C= (A/B)*100 A. The number of OBC requests for which the Supplier is responsible which are implemented successfully and within the stated timeframe for the Service Period. B. The total number of service requests that the Supplier is responsible for implementing that are raised for the Service Period. C. The percentage of OBC requests for which the Supplier is responsible, which are implemented successfully and within the stated time frame for that specific request for the Service Period.	99% of request delivered to the specified timescale	<99% <95%	1.0% 2.0%	Extended Support Hours 08:00 - 20:00 Monday - Friday 08:00 - 16:00 Saturday – Sunday	Monthly
EUC-BR-ENG-06	Engineering - Branch	Branch Customer Satisfaction net promoter score	Branch End users response rating when surveyed after closure of a incident or request ticket that rated their experience between: 10-9 Excellent to very good 8-7 Good to satisfactory 6-1 disappointing to poor	The Net Promoter Score is the % of responses during the reporting period that when achieved a score between 10-8 (promoter) subtracted by the percentage that achieve a score between 4-1 (detractors)	NPS <30 for the reporting period	<30 <10	1.0% 2.0%	Monthly	Monthly

POL00337657

EUC-BR-ENG-07	*Engineering*	*Repeat Failures*	*Any individual Branch that experienced 3 incidents raised for the same CI within a 30 days rolling period*	*Incidents raised against the same Branch CI within 30 days from the first incident being raised*	*3 CI failures within 30 days*	*3 CI incidents per 30 day period* *>3 CI incidents per 30 day period*	0.5% 1.0%	*30 day rolling period*	*Monthly*
EUC-ENG-DRP-01	Engineering	Device Replacement	The percentage of Incident replacement hardware requests dispatched by service type: Postal Service Next day Service Postal Service 48hr Service	C= (A/B)*100 A. The number of next day and 48hr postal requests allocated to the supplier dispatched on time B. The total number of next day and 48hr postal request allocated to the supplier C. The percentage of next day and 48hr postal request dispatched from the supplier	99% of items dispatched on time	<99% <95%	1.0% 2.0%	Extended Support Hours 08:00 - 20:00 Monday - Friday 08:00 - 16:00 Saturday – Sunday	Monthly
EUC-SM-REP-01	Service Management	Reporting	Governance and Service reports delivered complete within 5 Working Days of the end of the month:	Report upload into the customer repository C= (A/B)*100 A. The number of Governance and Service Reports delivered complete within the specified timescale for the Service Period. B. The total number required Governance and Service Reports delivered complete within the specified timescale for the Service Period. C. The percentage of required Governance and Service Reports delivered complete	99% within 5 Working Days of the end of the Service Period	<99% <95%	1.0% 2.0%	Business Hours	Monthly

POL00337657

				within the specified timescale for the Service Period					
EUC-SM-AS-01	Service Management	Asset management	Asset inventory accuracy	Accuracy of Asset inventory reports based on random 2% sample	99% accuracy of the total sample	<99% <95%	1.0% 2.0%	Business Hours	Monthly
EUC-SM-AS-02	Service Management	Asset management	Asset database updates	Update Asset register within 2 Working Days of a Asset installation	97% of assets updated within the defined period	<97% <90%	1.0% 2.0%	Business Hours	Monthly
EUC-SM-STK-04	Service Management	Stock Management	Repeat failures of any CI hardware that has failed more than 3 times in a rolling 30 day period	*Failure of the same Branch CI within 30 days from the first incident/failure being raised*	*3 CI failures within 30 days*	*3 CI incidents per 30 day period* *>3 CI incidents per 30 day period*	1.0% 2.0%	*30 day rolling period*	*Monthly*

POL00337657

EUC-SO-PM-01	Service Operations	Problem Management	Production of a Root Cause Analysis (RCA) report is completed for all P1 & P2 incidents within 3 working days of the incident	C= (A/B)*100 A. The number Root Cause Analysis Reports completed for all P1 and P2 Incidents within the specified timescale for the Service Period. B. The number of P1 and P2 Incidents for the Service Period. C. The percentage of required Root Cause Analysis Reports completed within the specified timescale for the Service Period	99% of RCA received by the customer within 3 days of the incident being raised	<99% of RCA received within 3 days <95% of RCA received within 3 days	1.0% 2.0%	Business Hours	Monthly
EUC-SO-PM-02	Service Operations	Problem Management	Production of a Root Cause Analysis (RCA) initial assessment is completed for all P1 & P2 incidents within 24hr of the incident	C= (A/B)*100 A. The number Root Cause Analysis initial completed for all P1 and P2 Incidents within the specified timescale for the Service Period. B. The number of P1 and P2 Incidents for the Service Period. C. The percentage of required Root Cause Analysis Reports completed within the specified timescale for the Service Period	99% of RCA initial assessments received by the customer within 1 day of the incident being raised	<99% of RCA received within 24hr <95% of RCA received within 24hrs	1.0% 2.0%	Business Hours	Monthly

POL00337657

EUC-SO-KM-01	Service Operations	Knowledge Management	Percentage of Knowledge Articles updated within 2 working days Note - on completion of the Shared Services separation this KPI will be split to represent colleague and branch services separately	Percentage of Knowledge Articles updated within 2 working days, where an inaccuracy has been identified by any party and reported to the Supplier C= (A/B)*100 A. The number Knowledge Articles updated within the specified timescale, where an inaccuracy has been identified by any party and reported to the Supplier, for the Service Period. B. The number Knowledge Articles inaccuracies reported by any party to the Supplier, for the Service Period. C. The percentage of Knowledge Articles updated within the specified timescale, where an inaccuracy has been identified by any party and reported to the Supplier, for the Service Period.	99% within 2 Working Days	<99% <95%	1.0% 2.0%	Business Hours	Monthly
EUC-SO-CM-01	Service Operations	Change Management	Percentage of Emergency Change Requests categorised as emergency, in the last Service Period in Production Note - on completion of the Shared Services separation this KPI will be split to represent colleague and branch services separately	C = (A/B)*100 A. The number of Emergency Change Requests implemented in the Service Period. B. The total number of Change Requests implemented in the Service Period. The percentage of Emergency Change Requests to overall Change Requests.	95% of changes not flagged as Emergency	95% 90%	1.0% 2.0%	24 x 7	Monthly

POL00337657

EUC-SO-CM-02	Service Operations	Change Management	Percentage of Failed Change Requests in the last Service Period Note - on completion of the Shared Services separation this KPI will be split to represent colleague and branch services separately	C = (A/B)*100 A. The number of Change Requests failed implemented in the Service Period. B. The total number of Change Requests implemented in the Service Period. The percentage of failed Change Requests to overall Change Requests.	99.5%	99.5% 98%	1.0% 2.0%	24 x 7	Monthly
EUC-SO-PM-01	Service Operations	Problem Management	Percentage of open problems tasks that are over 4 weeks old that have been assigned to the customer Note - on completion of the Shared Services separation this KPI will be split to represent colleague and branch services separately	C = (A/B)*100 A. The number of open problems that are over 4 weeks old and not dependent on another Supplier or the Customer. B. The total number of open problems that are not dependent on another Supplier or the Customer. The percentage of open problems over 4 weeks old and not dependent on another Supplier or the Customer.	90% problem tasks under 4 weeks old	90% 75%	1.0% 2.0%	Business Hours	Monthly

POL00337657

EUC-SO-PM-02	Service Operations	Problem Management	Percentage of open problems that are over 3 months old that are assigned to the supplier Note - on completion of the Shared Services separation this KPI will be split to represent colleague and branch services separately	C = (A/B)*100 A. The number of open problems that are over 3 months old and not dependent on another Supplier or the Customer. B. The total number of open problems that are not dependent on another Supplier or the Customer. The percentage of open problems over 6 months old and not dependent on another Supplier or the Customer.	95% problem tickets under 3 months old	<95% <90%	1.0% 2.0%	Business Hours	Monthly
EUC-IN-INC-05	Service Operations	Incident Management	Incident Update time for P1 and P2 Incidents in accordance with the target times set out below Every fifteen (15) minutes for Severity 1 unless otherwise agreed with Post Office Every thirty (30) minutes for Severity 2 unless otherwise agreed with Post Office Note - on completion of the Shared Services separation this KPI will be split to represent colleague and branch services separately	C = (A/B)*100 A. The number of incident tickets that were not updated in line with target times. B. The number of incident tickets that were updated in line with target times. The percentage of incident ticket updated in line with update target times	99% of tickets updated in line with response times	99% 95%	1.0% 2.0%	24 x 7	Monthly

POL00337657

EUC-SO-AGE-01	Service Operations	Aged tickets Colleague	Aged tickets as a total percentage of tasks allocated to the supplier for all tickets Note - on completion of the Shared Services separation this KPI will be split to represent colleague and branch services separately	C = (A/B)*100 A. The number of active Incident tasks which are allocated to the supplier which have missed their SLA and are older than 7 days . B. The total number of active Incident tasks allocated to the supplier which missed SLA C. The percentage of aged active Incident tasks allocated to the Supplier which are older than 7 days	95% of all tasks closed within 7 days of the SLA	<95% <90%	1.0% 2.0%	Extended Support Hours 08:00 - 20:00 Monday - Friday 08:00 - 16:00 Saturday – Sunday	Monthly
EUC-SO-CM-01	Service Operations	Change Management RFC closures	Update and closure of a RFC within 24hr of the completion, withdrawal or failure of the implementation Note - on completion of the Shared Services separation this KPI will be split to represent colleague and branch services separately	C = (A/B)*100 A. The number of RFC closed within 24hr of the implementation time stated within the RFC B. The total number of RFC assigned to the Supplier C. The percentage of RFC closed within 24hr of the implementation time stated within the RFC.	< 95% of all RFC closed within 24hr of the implantation time	<95% <90%	1.0% 2.0%	Extended Support Hours 08:00 - 20:00 Monday - Friday 08:00 - 16:00 Saturday – Sunday	Monthly
EUC-SO-IMAC-01	Service Operations	IMACD non-urgent	Percentage of Install, Move, Add and Change Dispose (IMACD) requests completed and closed within specified timescales that are not recorded as urgent Note - on completion of the Shared Services separation this KPI will be split to represent colleague and branch services separately	C = (A/B)*100 A. The number of IMACD requests completed by the Supplier and closed successfully within the specified timescale for the Service Period. B. The total number of IMACD requests that are allocated to the supplier for the Service Period.	95% of request completed within 2 working days	<99% <95%	1.0% 2.0%	Extended Support Hours 08:00 - 20:00 Monday - Friday 08:00 - 16:00 Saturday – Sunday	Monthly

POL00337657

				C. The percentage of non-urgent IMACD requests which are successfully completed and closed within 2 working days.					
EUC-SO-IMAC-02	Service Operations	IMACD urgent	Percentage of Install, Move, Add and Change Dispose (IMACD) request completed and closed within specified timescales that are not recorded as urgent Note - on completion of the Shared Services separation this KPI will be split to represent colleague and branch services separately	C = (A/B)*100 A. The number of IMACD requests completed by the Supplier and closed successfully within the specified timescale for the Service Period. B. The total number of IMACD requests that are allocated to the supplier for the Service Period. C. The percentage of non-urgent IMACD requests which are successfully completed and closed within the specified timescale.	95% of request completed within 8 Working Hours	<99% <95%	1.0% 2.0%	Extended Support Hours 08:00 - 20:00 Monday - Friday 08:00 - 16:00 Saturday – Sunday	Monthly

POL00337657

EUC-IN-INC-06	Service Operations	Priority Level 1 & 2 Incident Response Time	The percentage of all Priority 1 & Priority 2 Incidents that are allocated to the supplier and acknowledged within the specified timeframe (10 minutes) or identified by the supplier either by a event, alerting platform or other method that informs of a degradation or outage of service that corresponds to a Priority 1 or Priority 2 incident definition, the incident must be raised and the customer informed within the specified timeframe (10 minutes) Note - on completion of the Shared Services separation this KPI will be split to represent colleague and branch services separately	C= (A/B)*100 A. The sum of all Priority 1 & Priority 2 Incidents allocated to the correct Resolver Group (either supplier or customer) within the specified timeframe during the Service Period. B. The total number of Priority 1 & Priority 2 Incidents in the Service Period. C. The percentage of Priority 1 & Priority 2 Incidents correctly allocated to the correct Resolver Group (either supplier or customer) within the specified timeframe.	99% within 10 Minutes	<98% <95%	1.0% 2.0%	24 x 7	Monthly
EUC-IN-INC-07	Service Operations	Priority Level 3 Incident Response Time	The percentage of all Priority 3 Incidents that are allocated to the supplier and acknowledged with in the specified timeframe (30 minutes) or identified from the supplier either by a event, alerting platform or other method informs of a degradation or outage of service that corresponds to a Priority 3 incident definition, the incident must be raised and the customer informed within the specified timeframe (30 minutes) Note - on completion of the Shared Services separation this KPI will be split to	C= (A/B)*100 A. The sum of all Priority 3 Incidents allocated to the correct Resolver Group (either supplier or customer) within the specified timeframe during the Service Period. B. The total number of Priority 3 Incidents in the Service Period. C. The percentage of Priority 3 Incidents correctly allocated to the correct Resolver Group (either supplier or customer) within the specified timeframe.	98% within 30 Minutes	<98% <95%	1.0% 2.0%	Extended Support Hours 08:00 - 20:00 Monday - Friday 08:00 - 16:00 Saturday – Sunday	Monthly

POL00337657

			represent colleague and branch services separately						
EUC-INF-DR-01	Infrastructure	Disaster Recovery	The restoration of services during a disaster recovery invocation	Time taken to fulfil a complete or partial system restore from backup in line with the defined RPO	99% restoration of services in line with RPO	<99% <95%	1.0% 2.0%	24x7	Monthly
EUC-INF-DR-02	Infrastructure	Disaster Recovery	The restoration of services during a disaster recovery invocation	Time taken to restore a system to a disaster recovery status in line with the defined RTO	99% restoration of services in line with RTO	<99% <95%	1.0% 2.0%	24x7	Monthly
EUC-INF-BS-01	Infrastructure	Back up Services	For all in scope infrastructure services that require a scheduled Backup scheduled backup are completed to specified agreements	C= (A/B)*100 A. The number of expected backups completed within 24 hours of schedule B. The total number of expected backups C. Percentage of all expected backups have been scheduled.	95% of backups completed within 24hr	<95% <90%	1.0% 2.0%	24x7	Monthly
EUC-INF-BS-03	Infrastructure	Back up Services	Number of Azure backup Services that either fail to backup or fail post checks and test requirements	The number of expected backups specified in the requirements that during a reporting period that fail	<1 in a month	<1 in a month <2 in a month	1.0% 2.0%	24x7	Monthly
EUC-INF-SS-01	Infrastructure	Shared Service Technology	The individual resilient Wintel server pre-production Availability	The individual resilient Wintel server availability will operate at a level of Availability for 99% on a 24 x 7 basis	99% availability for the service period	<99% <97%	1.0% 2.0%	24 x 7	Monthly
EUC-INF-DR-03	Infrastructure	DR test plans	Provide test plans 10 Working Days before a scheduled DR exercise	The DR test plan upload into the customer repository at least 10 days prior to the exercise start date	100%	<100%	1.0% 2.0%	Business Hours	One off / Ad Hoc

POL00337657

EUC-INF-DR-04	Infrastructure	DR report	Provide a report within 5 Working Days of the DR exercise	The DR test report upload into the customer repository at least 5 days post the exercise start date	100%	<100%	1.0% 2.0%	Business Hours	One off / Ad Hoc
EUC-INF-DR-05	Infrastructure	DR test plans	Update quarterly Disaster recovery plans and process	The updated DR test plan upload into the customer repository on every quarter from the service commencement date	100%	<100%	1.0% 2.0%	Business Hours	Quarterly

Table 17: *EUC Key Performance Indicators*

POL00337657

8. TOOLING

This section provides information about the Post Office Colleague and Branch Tooling which is used to support the End User Computing service and are in scope of the supplier requirements of this agreement.

8.1 List of Tools

Tool	Description
ServiceNow ITSM Toolset	Post Office ServiceNow is to be used as the joint toolset between Post Office, the supplier and other managed service providers used by Post Office.
Branch Hub Portal	A ServiceNow driven IT Self-service interfaces for branches.
Web3 Purchase-to-Pay	Purchase-to-Pay e-sourcing solution used by Post Office.
CMDB Feed	A systems integration between the supplier CMDB to Post Office CMDB.
Monitoring feed(s)	A feed of monitoring events to the Post Office Splunk monitoring collector.
Security log shipping	A SIEM feed of security logs and events to the Post Office SIEM collector.

Table 18: *List of Tools*

8.1.1 ServiceNow

The Post Office Service Management team perform the role of Service Integrator and orchestrate services between themselves and third-party suppliers, with their IT Service Management tool of choice, ServiceNow.

For EUC services the primary Service Management processes that are used in the ServiceNow toolset include, but are not limited to:

- **Incident Management** – for the assignment and escalation of support tickets for user issues and break fix.
- **Change Management** – to ensure that changes with the Post Office IT ecosystem are managed and controlled.
- **Problem Management** – to investigate the root cause of user's issues and provide fixes and work arounds.
- **Request Management** – the fulfilment of user's requests for services that have been raised via the Self-Service portal.
- **Configuration Management** – hardware and software asset management and appropriate status accounting.

It should be worth noting that there are other modules within ServiceNow that are used by Post Office that are outside of the scope of EUC services such as Customer Service Management (CSM) which is used for Post Offices own case management for Branch.

ServiceNow also provides a Self-Service portal showing the status of services as well as the ability for a user to:

- Report an Issue
- Initiate 'chat' with a member of the Post Office Service Desk
- Access the Service Catalogue to request services
- Find Answers, by browsing the knowledge base

POL00337657

The new EUC supplier will use the Post Office ServiceNow toolset directly as well as using the new Field Service module in the delivery of their services, which will:

- Remove the need for complex integrations between toolsets
- Ensures that Post Offices processes are adhered too
- Simplifies reporting
- Provides clarity and visibility to all parties
- Standardises data formats and naming conventions

The EUC Suppliers should refer to the following onboarding guide:
Appendix A: Ref Doc- 010 EUC ServiceNow Supplier Onboarding Guide

8.1.2 Branch Hub Portal

The Post Office originally relied on traditional channels for the interactions between its Branch network and Back Office functions. Branch Hub was initiated to deliver a new digital self-service channel on the ServiceNow platform accessed by Branches through a web browser.

The aim of Branch Hub is to provide a central point of information and services which help Postmasters to manage and run their businesses more efficiently and conveniently. Through Branch Hub we simplify, speed up and bring consistency to some of our day-to-day processes.

It is intended to make it more convenient and easier for Postmasters and their teams to complete tasks, process orders, and receive updates from the business. We've listened and responded to feedback from Post Offices and are invested in this new technology to help make it easier for Postmasters. As customer's' needs are changing all the time, we need to make sure we continue to exceed expectations by introducing additional new convenient ways to speed up and streamline processes for Postmasters, freeing up their time to run their business more efficiently and delivering great customer-service.

Branch Hub was launched in April 2020 to support Post Office's response to the COVID 19 pandemic, including functionality to change of branch hours, agent remuneration and PPE ordering. This drove adoption to surpass 9,400 End Users by July 2020. The delivery of further features Planned orders, Stock and Coin ordering, has been rolled out since the summer and is being adopted by branches on an ongoing basis. Today there are 9,325 branches and 12,493 End Users using the system. These features, once adopted by branches on the Branch Hub platform, are then decommissioned on the Horizon Point of Sale system.

Currently the business is revisiting the vision and future roadmap of product deliverables. Therefore, any Collateral relating to End User Branch devices e.g., Knowledge Articles, incidents, requests, FAQs etc. related to Branch Kit will need to be actioned and maintained by the Supplier.

8.1.3 Web3 Purchase-to-Pay

Web3 is the Post Office e-sourcing solution, used for all purchase-to-pay capabilities with all Suppliers of the Post Office. Web3 allows the Post Office to:

- Run tenders
- Manage contracts

POL00337657

- Raise Requisitions / Purchase Orders
- Process and manage invoices
- Track spend against contracts

8.1.4 CMDB Feed

The purpose of a CMDB is to provide accurate and reliable information about Post Office digital services and the infrastructure that supports them. The CMDB is used by Post Office teams to identify out what's wrong and get our services back up and running quickly, correctly allocate incidents, and to track and control operational change.

The CMDB is delivered via the ServiceNow platform and is configured to show infrastructure relationships, service topologies, change histories, software versions and more. CI classes are arranged in a class hierarchy, with each subclass extending the attributes of its parent class. Within the Post Office we typically use three tiers with a business service supports a business capability, such as our point of sale capability, and is consumed by business users. Business services are typically underpinned by one or more application services like the point of sale application. Lastly a technical service is a technical capability that underpins one or more application services, for instance the hardware used to on the counter to deliver the services.

Understanding the relationship between service CIs and supporting infrastructure CIs is critically important. For instance, it helps Post Office support teams to diagnose the root cause of service issues. A service map in the CMDB captures these relationships, showing which CIs support the service and how they are related to other CIs to quickly resolve fault paths and assess impact.

The Post Office CMDB is populated via integrations with our key suppliers to create a holistic view of our end to end services, distribution of assets, relationship and attributes. The EUC Supplier will (as per the requirements) integrate into the Post Office CMDB ensuring the integrity of Business Services and business context. The EUC Supplier Configuration Management service will support the Post Office on its service-oriented approach to IT management.

8.1.5 Security

Summary for Security Operations Integrations to 3rd parties:
Collecting logs or notable events is in the scope across all scenarios. Our preferred method is to allow digest and correlation of all security logs in the native environment, such as Azure Security Centre. Notable events are then collected via an API in to our SIEM platform. On scenarios where API is not possible, we would require integration through Universal Forwarders.

Incident response:
Post Office SOC will be integrated to any and all cyber incidents with 3rd parties from a second line of defence perspective. Access Management, PAM, MIM Incidents shall be fully integrated with Post Office SOC with the ability for SOC to respond efficiently.

Event collection for enterprise analysis:
All devices, (PC's, Servers, network devices, AV's, etc) report security-critical events to audit and monitor services in line with Post Office IT Security operations coverage requirements.

- Service providers shall maintain logs of all key events (including but not limited to audit logs, security logs and other security events), coverage in line with industry standards and frameworks such as MITRE ATT&CK framework.

POL00337657

- Effective and efficient integration of all security logs must be digestible at source by native security capabilities, such as Azure Security Centre, AWS Sec Hub. These logs then must be available to be transferred to a single pane of glass SIEM platform.

SOC usable space, sandbox and permissions:

- Post Office SOC must have correct level of permissions to conduct their duties effectively in line with Access Management business policies and need to know privileges
- Necessary workspace on cloud systems is necessary to conduct tests, labs or sandbox analysis.
- Correct level access must be provided to all SOC tool integrations with necessary components of the platform to enable automation, through Threat Intel ingest, ServiceNow SecOps incident response workflow, SOAR functions.
- Flexibility must exist to accommodate and assist with other SOC requirements, so to satisfy risk averse appetite for Post Office, in particular where new techniques evolve to improve security.

POL00337657

9. IMPLEMENTATION

9.1 Implementation Overview

Implementation is the period of time when the EUC Supplier will build, test and implement its solution and perform all the activities necessary to replace the existing services.

The Implementation period starts on the date of contract commencement and ends when the final Implementation milestone has been achieved and signed off by Post Office. At this stage the Run services will be delivered by the EUC.

9.2 Implementation Objectives

During the Implementation period the Supplier should always ensure that:

- They endeavour to minimise disruption or degradation of any existing production services.
- Ensure that services are tested, validated & approved as per to the project test strategy, prior to being moved into live service.
- Adhere to Post Offices service transition management process so that services can be cut over at agreed points of time that align to the Implementation plan and Milestone dates.
- Minimise Implementation costs to Post Office where appropriate to do so.
- Engage in building a collaborate relationship with Post Office and other suppliers for the duration of the Implementation and continue to do so after Implementation.

9.3 Implementation Principles

The EUC Supplier shall perform all agreed activities to be in a position to be able to deliver Services. Successful Implementation is dependent upon co-operation with all parties, including Post Office and other suppliers, and that the EUC Supplier shall comply with this approach.

Individuals with appropriate skills and experience shall be provided by the EUC Supplier for the project management and delivery of the Implementation.
Implementation plans, designs and documentation shall be created and maintained by the EUC Supplier throughout the life cycle of the Implementation and be made available to any party where required.

9.4 Implementation Services

The Implementation lifecycle shall comprise of four distinct phases and the EUC Supplier should base their plans accordingly:

- Phase 1 - Initiation
- Phase 2 - Design
- Phase 3 - Build, test & deliver
- Phase 4 - Acceptance

The Implementation shall be delivered by the EUC Supplier by a series of projects or workstreams. Each project shall have a supplier project manager, unless agreed otherwise with Post Office. During the Implementation, the EUC Supplier shall:

- Implement its solution in such a way that it meets Milestone dates and acceptance criteria.
- Deliver services post service commencement date which meets the agreed service levels and KPIs
- Co-operate with all third parties whose services are relevant to the implementation.

POL00337657

- During the implementation be compliant to all Post Office security policies and standards.
- Communicate to Post Office as quickly as possible should:
    - The supplier believe that they will miss an agreed Milestone date or deliverable.
    - A dependency cannot be achieved by a supplier or itself.
    - Any other risk be identified that will prevent the delivery of a Milestone to the agreed timelines.
- An Implementation table that lists all Milestones & Milestone payments can be found in the order form.
- The EUC Supplier Implementation plan shall incorporate all Milestones that are listed in the Implementation table.

9.5 Implementation Delivery Approach

Progress of the EUC Supplier during Implementation shall be measured against the Milestones incorporated in the Implementation Plan.

9.6 Implementation & Integration

The EUC Supplier shall accept that detailed planning is essential for the successful Implementation of services. Within the Implementation Plans, the EUC Supplier shall incorporate Milestones and their dates and their proposed implementation dates for the following:

- The Milestones that are listed in the Milestone Table.
- Testing period and expected completion of testing.
- Any end user training and deployment activities.
- Listing of the detailed activities that will need to occur to achieve each Milestone.
- A RACI for all parties involved in the Implementation.
- Any dependencies that have been identified.
- The output of an impact assessment of any other projects or changes that are occurring in the Post Office landscape during the Implementation time frame.

9.7 Service Operation

Prior to Service Commencement, the EUC Supplier will need to ensure that an organization is in place to deliver the new Services and as a minimum should include:

- Role descriptions and RACI.
- The appropriate recruitment and staffing of resource to deliver Service.
- Process, procedures and tooling, including their validation and assurance.

During the Implementation period the EUC Supplier will need to stand up the process and capabilities in order for them to deliver Services. This should include as a minimum:

- The processes for billing and invoicing as well as any other financial management process that are required.
- Plans for staff, including any rosters and rotas to cover extended days or weekend shifts.
- Reporting, for service levels, assets, etc.
- Confirming access to Post Offices physical locations and sites
- Time sheeting capability so that effort on a time and material basis can be recorded correctly.
- Securing the various technical accounts and delegation of authority roles that are required to access Post Office IT systems.

POL00337657

9.8 Change

During the Implementation period, the Supplier shall observe the services that are being delivered other suppliers and confirm to Post Office as soon as possible if any changes to these services by any supplier during the Implementation period will have an impact on the EUC Supplier to meet any of their Milestone commitments. Should this occur, then the EUC Supplier shall provide Post Office with an impact assessment.

9.9 Process & Procedures

The EUC Supplier will collaborate with Post Office, other suppliers and any third parties in the agreement and creation of the processes and procedures that will be used to deliver Services. These will then be implemented and operated in alignment with Post Office s policies and standards.

Delivery, management and reporting of services by the EUC Supplier shall be facilitated via the agreed processes and procedures and this shall include as a minimum:

- End to end operating models that identify who is responsible for each element of the service including support and management as well as the technical aspects.
- The demarcation points and end to end process between the EUC Supplier and other third parties.
- Reporting mechanisms, to measure performance against agreed Service Levels.

Post Office will expect to review the processes and procedures and to approve them. The EUC Supplier shall also work with any third party on their processes and procedures that will become impacted or require amendment as a result of the Implementation of the Services. Within the Implementation Plan, the EUC Supplier shall ensure enough time has been allocated for the creation, review and approval cycle for all of these processes and procedures.

9.10 Security

A Security Management Plan shall be developed by the EUC Supplier and provided to Post Office for review and approval 20 working days following contract signature. Should the EUC Supplier identify any risks that a service could be impacted as a result of Implementation, then the EUC Supplier shall provide a plan to manage these risks and update the Security Management Plan as appropriate. Detailed requirements for the Security Management Plan can be found in **RM3804-Alternative-and-additional-tc-v4, Schedule E Security Requirements**.

9.11 Business Continuity & Disaster Recovery

Business Continuity & Disaster Recovery Plans shall be developed by the EUC Supplier and provided to Post Office for review and approval 20 working days following contract signature. Post Office is in the process of migrating EUC infrastructure to the Post Office Azure environment and is reviewing the recovery targets for the services included. These Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) will be provided to the EUC Supplier at contract signature.
Detailed requirements for the Business Continuity & Recovery Plans can be found in **RM3804-Alternative-and-additional-tc-v4, Schedule B1 Business Continuity And Disaster Recovery**.

9.12 Transition of Staff (Relevant Transfers)

Within the Implementation Plan, where required the Supplier shall include all activities related to any staff transfer (Relevant Transfers) including staff consultations,

POL00337657

communications etc, and shall conduct the transfer pursuant to the requirements of **RM3804-Alternative-and-additional-tc-v4, Part B of Call Off Schedule A3 (Staff Transfer).**

Further details of the scope of staff at risk can be found in the Appendix A document **Ref Doc-011-Tupe List v1**. The document is password protected and will be provided to suppliers responding to the tender.

9.13 Business Communications

During the Implementation the EUC Suppler will collaborate with Post Office in the creation of a strategy and plan to communicate to the business user community. Any communication materials that are required shall be created by the EUC Supplier in conjunction with Post Office and must approved by Post Office prior to any publication.

9.14 Implementation Governance

To ensure there is governance and transparency between all parties during the Implementation the following governance meetings and boards shall be scheduled with the expectation that all invitees will be present and attend.

Meeting	Frequency	Purpose	Attendees
EUC Implementation Status	Weekly	To review: • Progress of Implementation via a status report. • Current risks and issues. • Any blockers or items that need to be escalated to the program board.	• Post Office EUC Supplier
EUC Supplier Implementation Board	Fortnightly	Allows all parties to provide the status of the Implementation via a status report in a collaborative manner, to review progress of the implementation and any current dependencies between suppliers.	• Post Office EUC Supplier • Other suppliers as required

Table 19: *Governance meetings*

In addition to these tabled governance meetings there may be additional requirements for other ad-hoc meetings based on demand such as daily stand ups.

9.15 Reporting

The EUC Supplier during Implementation shall provide Post Office updates on its progress or lack of progress at regular frequencies and outlined in the Implementation Plan. The report shall show progress made each Milestone as well as showing the progress towards the completion of Implementation.

9.16 Supplier Implementation Team

Suitability qualified and experienced personnel shall be appointed by the supplier to manage and deliver the Implementation, most likely to include:

- Implementation Director, overall responsibility for the delivery of the Implementation by the Supplier.

POL00337657

- Implementation Manager(s), responsible for the day to day management of the Implementation.
- Workstream Managers, responsible for the detailed planning and execution of activities for their workstream.

9.17 Document Deliverables

The following document deliverables are required as a minimum for Service Implementation.

DELIVERABLE	DESCRIPTION	DELIVERY
High Level Plan PID & RAID	The artefacts that are required to kick off and initiate the Implementation project that is aligned to industry standard project methodology.	Contract Commencement +20 working days
Solution Overview	The overview of the Supplier's solution and what it will deliver.	Contract Commencement +20 working days
Security Management Plan	Outlining how the supplier will aim to ensure that all aspects of the service that they are delivering, and associated processes comply with Post Office Security Policies.	Contract Commencement +20 working days
Test Strategy	Describing the practise of testing within the implementation consistent with the Post Office Test Policy & any relevant supplier Test Policies.	Contract Commencement +20 working days
Project Requirements Specification	To ensure that the requirements specific to the Implementation are formally captured.	Contract Commencement +20 working days
BCDR Plan	Describing how the supplier will restore services in the event of a disaster and the activities required to support business process in providing business continuity.	Contract Commencement +20 working days
Quality Plan	Describing the activities, standards, tools and processes necessary to achieve the quality in the delivery of the implementation.	Contract Commencement +20 working days
Deliverables Matrix Document	A matrix for managing deliverables and their phases throughout the delivery of the project.	Contract Commencement +20 working days
Level 4 Detailed Plan	Detailed plan that shows resources assigned and detailed work activity.	Contract Commencement +20 working days
Asset & Volume Validation Assessment	Factual baselines for capacity planning	Contract Commencement +60 working days
Test Report (Colleague)	A summary of all testing activities and final test results for Colleague EUC services.	As per the agreed date in the Level 4 Detailed Plan

POL00337657

Test Report (Branch)	A summary of all testing activities and final test results for Branch EUC services.	As per the agreed date in the Level 4 Detailed Plan
Detailed Cut Over Plan (Colleague)	Containing the appropriate run books, scheduling and resourcing for cutting over EUC services for Colleague.	As per the agreed date in the Level 4 Detailed Plan
Detailed Cut Over Plan (Branch)	Containing the appropriate run books, scheduling and resourcing for cutting over EUC services for Branch.	As per the agreed date in the Level 4 Detailed Plan
Project Closure Report	Report to confirm that all objectives and deliverables have been met and handed over.	As per the agreed date in the Level 4 Detailed Plan

Table 20: *List of Document deliverables*

Product Description: Document Deliverable Matrix

Product Description	
Title of Deliverable	Documentary Deliverable Matrix (DDM)
Purpose of Deliverable	The EUC Supplier shall develop a complete list of document deliverables for the Implementation, mapped onto the project lifecycle/plan and as required to support project delivery. There are four primary uses of the document: ▪ To ensure that all deliverables required to support the delivery of the Implementation, as defined in the PID, are identified and agreed with all stakeholders ▪ To act as a base document against which the project can assess progress of agreed deliverables as they are mapped to the delivery lifecycle ▪ To determine the ownership of and level of assurance required to each product identified in the DDM ▪ To validate at project closure that deliverables have been delivered
Scope of Deliverable	The identified delivery Project
Format & Presentation of Deliverable	MS Excel
Composition of Deliverable	The EUC Supplier shall provide a DDM that identifies all deliverables required to support the delivery of the Implementation. This will be produced in the same format as the master DDM template retained by the Post Office. The master DDM lists all products that could be required at each stage of the delivery lifecycle. The EUC Supplier shall work with Post Office to determine which of the products listed are required for the Implementation, who will produce them and agree with Post Office the points at which documentation will be required and assurance levels i.e. is the document approved by Post Office. The DDM shall include the following information: ▪ Owner ▪ Document Category ▪ Document Name ▪ Identify Management or Specialist Product

POL00337657

	▪ Required Y/N ▪ Delivery Status (RAG) ▪ Document treatment and Lifecycle Status mapped across Post Office Lifecycle
Derivation of Deliverable	The Implementation specific DDM will be derived from: ▪ Post Office – Master DDM ▪ Post Office specified control requirements ▪ Additional information gathered during Project Initiation Stage ▪ Project management standards ▪ Post Office s specified control requirements
Allocated to	Owned by the EUC Supplier and Post Office EUC Implementation Project Manager Created by the EUC Supplier
Quality Criteria for Deliverable	The DDM must ensure that it: ▪ Identifies all document deliverables required throughout the Lifecycle of the Implementation ▪ Captures all Specialist products identified to complete the Project ▪ Includes Management products ▪ Reflects the deliverables identified in the schedules ▪ Complies with the Product Description. ▪ Represents an accurate and complete record of the project baseline
Quality Method	▪ Quality checked by the Post Office Programme as appropriate • Approved by the relevant project board identified in the Governance structure prior to submission to the Phase 1 – Initiation gate review • Approved by the Post Office PMO as part of the pre-Phase 1 – Initiation pre gate health check review
People or skills required	**Reviewers** ▪ Post Office EUC Implementation Project Manager ▪ Post Office Service Design Lead ▪ Post Office Architecture Lead ▪ Post Office EUC Re-procurement Programme Manager ▪ Other suppliers (as required) **Approval** ▪ Post Office Programme representatives, dependent on the stakeholders identified in the PID For info to ▪ Stakeholders ▪ Team Members
First Draft Delivery Date for Deliverable	Within 20 working days of project notification.
Planned Successful Approval Date for Deliverable	As per The Implementation

Table 21: *Documentary Deliverable Matrix (DDM) Produce Description*

Product Description: Level 4 Project Plan

Product Description	
Title of Deliverable	Level 4 Project Plan

POL00337657

Purpose of Deliverable	The EUC Supplier shall develop a complete set of Level 4 project plans for the Implementation which will contain the full set of activities required by a function within the project team structure e.g. architecture. The Level 4 plan is produced during the initiation phase of the project and should, collectively, form the end to end timeframe and activities required to deliver the project as defined in the PID. There are three main objectives of the Level 4 plan: ▪ To ensure that all elements of the Implementation as defined in the PID and associated deliverables as agreed in the DDM have been planned, resourced and can be delivered within the agreed project timeframes ▪ To act as a baseline document against which the project team can assess progress of the Implementation ▪ To ensure that any dependencies, whether they are external to the Implementation or internal between function groups, have been captured in the baseline plans agreed at the Phase 1 – Initiation gate
Scope of Deliverable	Implementation
Format & Presentation of Deliverable	MS Project 2010
Composition of Deliverable	The EUC Supplier shall provide a Level 4 plan that specifies all activities, dependencies, resource, effort and outputs required from the EUC Supplier, others suppliers and Post Office in order to achieve project milestones. The Level 4 plan will be produced in the same format as the template retained by Post Office to ensure that the Level 4 plan can be integrated by Post Office and the EUC Supplier into an end to end Implementation plan. • Timeframes, activities, resource, effort and dependencies identified in the Level 4 plan will be baselined at the Phase 1 – Initiation Gate review. Once the Implementation is in the execution phase, the baseline will be retained, and the Level 4 plan should show the forecast dates at all times. Changes required to the Level 4 plan following agreed baseline will be implemented in line with the governance structure as described in the change control process in the schedules.
Derivation of Deliverable	The Implementation specific Level 4 plan will be derived from: ▪ Post Office Framework Requirements ▪ EUC Supplier responses ▪ Other suppliers ▪ Post Office specified control requirements ▪ Additional information gathered during Project Initiation Stage ▪ Project management standards ▪ Post Office s specified control requirements
Allocated to	Owned by the EUC Supplier and Post Office EUC Service Implementation Project Manager Created by the EUC Supplier
Quality Criteria for Deliverable	The Level 4 plan must ensure that it: ▪ Identifies all document deliverables required throughout the Lifecycle of the Implementation ▪ Identifies all resource, effort, duration required throughout the lifecycle of the Implementation ▪ Captures all Implementation specific products ▪ Includes all delivery dependencies

POL00337657

	▪ Reflects the deliverables identified in the schedules ▪ Complies with the Product Description. ▪ Represents an accurate and complete record of the project baseline
Quality Method	▪ Quality checked by the Post Office Programme as appropriate ▪ Approved by the relevant project board identified in the Governance structure prior to submission to the Phase 1 – Initiation Gate review ▪ Approved by the Post Office PMO as part of the pre-Phase 1 – Initiation ▪ Gate health check review
People or skills required	**Reviewers** ▪ Post Office EUC Implementation Project Manager ▪ Post Office Service Design Lead ▪ Post Office Architecture Lead ▪ Post Office EUC Re-procurement Programme Manager ▪ Other suppliers (as required) **Approval** ▪ Post Office Programme representatives, dependent on the stakeholders identified in the PID For info to ▪ Stakeholders ▪ Team Members
First Draft Delivery Date for Deliverable	Within 20 working days of project notification.
Planned Successful Approval Date for Deliverable	As per the Implementation

Table 22: *Level 4 Project Plan Product Description*

Asset & Volume Validation Assessment

Product Description	
Title of Deliverable	Asset & Volume Validation Assessment
Purpose of Deliverable	The purpose of the Asset & Volume Validation Assessment is to present to Post Office for Approval, actual, historical and or assumed volumetric data to form the volume baselines as relevant to each service. These Asset & Volume data shall form the Asset & Volume baselines as relevant to each Service assumed at the Service Commencement Date. The Asset & Volume baseline data shall be used to update the base data for the EUC Supplier's capacity plan
Scope of Deliverable	Implementation
Format & Presentation of Deliverable	The Volume Baselines are to be: • Presented in an electronic format to be agreed with the Post Office • Version Controlled.
Composition of Deliverable	The Asset & Volume baseline data shall include, but not be limited to: • Numbers of users. • types of users. • Number of devices, including, but not limited to, PCs, laptops, tablets, printers, monitors and other peripherals. • Instances of software installed. • Number of software licences. • Infrastructure components, including servers, storage, network appliances • Application components, including servers, storage

POL00337657

Derivation of Deliverable	The Asset & Volume Baselines shall be derived from (where required to provide comprehensive information): ▪ Current Asset Inventories. ▪ Site Audits. ▪ Investigative Tools. ▪ Asset Registers;
Allocated to	Owned by the EUC Supplier and Post Office EUC Service Implementation Project Manager Created by the EUC Supplier
Quality Criteria for Deliverable	▪ Must conform, but not be limited, to the following: o Post Office EUC Programme Quality Standards ▪ Must support (as a minimum) Industry standard methodology; i.e: o ITIL; and o PRINCE2 Project Management Methodology.
Quality Method	▪ Quality checked by the Post Office Programme as appropriate ▪ Delivered to the format specified ▪ Complies with the Product Description ▪ Content reflects the proposed approach described in the Suppliers' Implementation Solution Descriptions and is in accordance with the Implementation Requirements.
People or skills required	**Reviewers** ▪ Post Office EUC Implementation Project Manager ▪ Post Office Service Design Lead ▪ Post Office Architecture Lead ▪ Post Office EUC Re-procurement Programme Manager **Approval** ▪ Post Office Programme representatives ▪ Post Office Architecture Lead For info to ▪ Stakeholders ▪ Team Members
First Draft Delivery Date for Deliverable	Within 60 working days of project notification.
Planned Successful Approval Date for Deliverable	As per the Implementation

Table 23: *Asset and Volume Validation Assessment Product Description*

Product Description: PID

Product Description	
Title of Deliverable	Project Initiation Document
Purpose of Deliverable	The Project Initiation Document (PID) defines all major aspects of the Implementation and forms the basis for its management and the assessment of overall success. It forms the 'contract' between the Implementation Team and corporate or programme management. The PID is produced during the initiation stage of the Implementation and should be read in conjunction with the Solution Overview, produced at the same time, which describes the overall solution to be delivered. There are three primary uses of the document:

POL00337657

	▪ To ensure that the Implementation has a complete and sound basis for proceeding before there is any major resource commitment to the Implementation ▪ To act as a base document against which the Project can assess progress, change management issues, and ongoing viability questions. ▪ Provide a single source of reference about the Implementation so that people joining the 'temporary organisation' can quickly and easily find out what the Implementation is about, and how it is being managed.
Scope of Deliverable	Implementation
Format & Presentation of Deliverable	It is expected that all PIDs will be produced in OpenDocument format, PDF, or, as an exception, DOCX where particular features are unsupported
Composition of Deliverable	The EUC Supplier shall provide a PID that defines the Implementation within the Post Office EUC Re-procurement Programme. The PID includes all of the planning components that address scope, budget, schedule, quality, configuration management, risks, issues and performance monitoring. The PID shall include the following Sections: DOCUMENTATION CONTROL ▪ Version Control ▪ Reviewers ▪ Approvals ▪ Referenced Documents INTRODUCTION ▪ Purpose of This Document ▪ Background PROJECT DEFINITION ▪ Project Overview ▪ Project Objectives ▪ Project Scope ▪ Project Deliverables / Outcomes ▪ Project Exclusions/Constraints/Interfaces PROJECT APPROACH ▪ Delivery Overview ▪ Solution Overview ▪ Critical Success Factors PROJECT RISKS PROJECT TIMEFRAMES PROJECT ORGANISATION ▪ Overview ▪ Project Organisation Structure ▪ Project Roles and Responsibilities PROJECT COMMUNICATIONS PLAN ▪ Overview ▪ Project Stakeholder Contact List ▪ Project Communication Matrix PROJECT QUALITY PLAN ▪ Overview ▪ Purpose ▪ Acceptance Criteria PROJECT PLAN ▪ Overview ▪ Plan Prerequisites

POL00337657

	▪ Project Dependencies ▪ Planning Assumptions PROJECT MANAGEMENT PROCEDURES ▪ Governance ▪ Project Controls ▪ Project Reporting ▪ Project Assurance ▪ Project Tolerances ANNEXES ▪ Glossary
Derivation of Deliverable	Derivation of Deliverable. The PID will be derived from: ▪ Post Office – Contract for the Provision of EUC services ▪ EUC Supplier Tender response ▪ Post Office specified control requirements ▪ Additional information gathered during Project Initiation Stage ▪ Project management standards ▪ Post Offices specified control requirements ▪ Solution Overview
Allocated to	Owned by the Supplier and Post Office EUC Implementation Project Manager Created by the EUC Supplier
Quality Criteria for Deliverable	The PID must ensure that it: ▪ Supports (as a minimum) Industry standard methodology; i.e., Prince 2, MSP ▪ Reflects the proposed approach described in the Solution Overview and is in accordance with the Post Office requirements for the Project ▪ Complies with the Product Description. ▪ Represents an accurate and complete record of the Project baseline
Quality Method	▪ Quality checked by the Post Office Programme as appropriate ▪ Approved by the relevant project board identified in the Governance structure prior to submission to the Phase 1 – Initiation Gate review ▪ Approved by the Post Office PMO as part of the pre-Gate Phase 1 – Initiation health check review
People or skills required	**Reviewers** ▪ Post Office EUC Implementation Project Manager ▪ Post Office Service Design Lead ▪ Post Office Architecture Lead ▪ Post Office EUC Re-procurement Programme Manager ▪ Other suppliers (as required) **Approval** ▪ Post Office Programme representatives, dependent on the stakeholders identified in the PID **For info to:** ▪ Stakeholders ▪ Team Members ▪ Other Suppliers
First Draft Delivery Date for Deliverable	Within 20 working days of project notification.

POL00337657

Planned Successful Approval Date for Deliverable	As per the Implementation

Table 24: *PID Product Description*

Product Description: Project Requirements Specification

Product Description	
Title of Deliverable	Project Requirements Specification (PRS)
Purpose of Deliverable	The Project Requirements Specification is produced during Feasibility or Initiation stages of the Post Office ICT delivery lifecycle and is baselined within the Initiation stage. Its purpose is to ensure that the requirements specific to the Implementation project are formally captured; and are in a fit state to take forward a business change initiative, a process re-engineering activity or develop the technical design specification for an IT solution. The Project Requirements Specification should be read in conjunction with the Solution Overview.
Scope of Deliverable	This document should: ▪ State (via reference not repetition) the Call Off Schedule Service Levels, Service Credits and Performance Monitoring Part A Service Requirements that will be met by the Project ▪ Capture any constraints to the scope of applicability of the 2 Part A Requirements (e.g. if the Project is a particular iteration aimed at only one business area). ▪ Reference any Policies, Processes Procedures; architecture principles and known issues that the Project is intended to satisfy / remediate. ▪ Capture any detailed business and service requirements that are needed to supplement the Call Off Schedule Service Levels, Service Credits and Performance Monitoring Part A Service Requirements. ▪ Capture any derived service requirements (e.g. non-functional requirements, security requirements). ▪ The Project Requirements Specification will be a key artefact in evidencing acceptance into service.
Format & Presentation of Deliverable	It is expected that all Project Requirements Specifications will be produced in OpenDocument format, PDF, or, as an exception, DOCX where particular features are unsupported.
Composition of Deliverable	▪ Introduction ▪ Background ▪ Objective ▪ Scope ▪ Approach ▪ Constraints ▪ Business Process Functional requirements – grouped by type/category as appropriate Non-functional requirements – containing, as a minimum, the following categories. Further categories will be dependent on the type of solution being designed: ▪ Performance ▪ Accessibility ▪ Availability ▪ Back up ▪ Interoperability ▪ Scalability ▪ Capacity

POL00337657

	▪ Security ▪ Appendices (if applicable) ▪ Requirements Traceability Matrix
Derivation of Deliverable	▪ Supplier Solution ▪ Call Off Schedule Service Levels, Service Credits and Performance Monitoring Part A (Service Requirements) ▪ Call Off Schedule Service Levels, Service Credits and Performance Monitoring Part B (Service Performance Management)
Allocated to	Owned by the EUC Supplier and Post Office EUC Implementation Project Manager Created by the EUC Supplier
Quality Criteria for Deliverable	▪ Delivered to the format specified ▪ Alignment to the PID and Solution Overview ▪ Traceability to contracted (Schedule) requirements
People or skills required	**Reviewers** ▪ Post Office EUC Implementation Project Manager ▪ Post Office Service Design Lead ▪ Post Office Architecture Lead ▪ Post Office EUC Re-procurement Programme Manager **Approval** ▪ Post Office Programme representatives, dependent on the stakeholders identified in the PID For info to ▪ Post Office Programme
First Draft Delivery Date for Deliverable	Within 20 working days of project notification.
Planned Successful Approval Date for Deliverable	As per the Implementation

Table 25: *Project Requirements Specification (PRS) Product Description*

Product Description: Business Continuity & Disaster Recovery Plan

Product Description	
Title of Deliverable	Business Continuity & Disaster Recovery (BCDR)
Purpose of Deliverable	The BCDR Plan shall detail the processes and activities which the EUC Supplier shall follow to ensure continuity of the business operations and process following any disruption or failure of any element of the EUC Services and the recovery of EUC Services in the event of an actual disaster.
Scope of Deliverable	1.
Format & Presentation of Deliverable	It is expected that all Project Requirements Specifications will be produced in OpenDocument format, PDF, or, as an exception, DOCX where particular features are unsupported.
Composition of Deliverable	▪ Introduction ▪ Background ▪ Objective ▪ Scope ▪ Approach ▪ Plan Invocation

POL00337657

	▪ Communication ▪ Roles & Responsibilities ▪ Testing ▪ Critical Success Factors & Key Performance Indicators ▪ Regulatory Compliance ▪ Business Impact Assessment ▪ Process Objective & Scope ▪ High Level Process Descriptions ▪ ITSCM Sub-process work instructions ▪ Detailed list of primary systems including RTP & RPO
Derivation of Deliverable	▪ EUC Service Description (Service Requirements) ▪ Post Office Technical Reference Documentation ▪ RM3804-Alternative-and-additional-tc-v4, Schedule B1 Business Continuity And Disaster Recovery ▪ Post Office BCDR/ITSC Plans & Policies (**Note:** With the migration of EUC infrastructure to the Post Office Azure environment Post Office is reviewing the BCDR/ITSC Plans and Policies, including Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) for the EUC Services. These documents will be provided to the EUC Supplier at contract signature to input in to the required EUC Supplier Disaster Recovery Plan).
Allocated to	Owned by the EUC Supplier and Post Office EUC Implementation Project Manager Created by the EUC Supplier
Quality Criteria for Deliverable	▪ Delivered to the format specified ▪ Alignment to the PID and Solution Overview ▪ Traceability to contracted (Schedule) requirements
People or skills required	**Reviewers** ▪ Post Office EUC Implementation Project Manager ▪ Post Office Service Design Lead ▪ Post Office Architecture Lead ▪ Post Office EUC Re-procurement Programme Manager **Approval** ▪ Post Office Programme representatives, dependent on the stakeholders identified in the PID
First Draft Delivery Date for Deliverable	Within 20 working days of project notification.
Planned Successful Approval Date for Deliverable	As per the Implementation

Table 26: *Business Continuity and Disaster Recovery Plan Product Description*

Product Description: Solution Overview

Product Description	
Title of Deliverable	Solution Overview (SO)
Purpose of Deliverable	The Solution Overview is produced during Feasibility or Initiation stages of the Post Office ICT delivery lifecycle and is baselined within the Initiation stage. Its purpose is to present a common understanding of the solution to be delivered prior to entering the Design phase of the Project. It should be read in conjunction with the PID, produced at the same time, which describes the approach that will be taken to deliver the solution.

POL00337657

Scope of Deliverable	The Solution Overview will describe the solution at a conceptual and logical level, addressing service design, architecture and information assurance dimensions. The scope will be constrained to provide an overview of the services explicitly delivered by the delivery Project.
Format & Presentation of Deliverable	It is expected that all Solution Overviews will be produced in OpenDocument format, PDF, or, as an exception, DOCX where particular features are unsupported.
Composition of Deliverable	All solution documentation should be properly titled, and version controlled. Composition of Deliverable. The Solution Overview shall include the following Sections: Introduction ▪ Purpose ▪ Scope ○ Specific Inclusions ○ Specific Exclusions ▪ Background ▪ Summary Requirements ▪ Business Requirements ▪ Service Functional Requirements ▪ Service Level Requirements ▪ Service Operational and Management Requirements ▪ Service Applicability ▪ Service Contacts Assumptions, Risks, Dependencies and Constraints ▪ Assumptions ▪ Risks ▪ Dependencies ▪ Constraints Service Design and Topology ▪ Service Architecture ▪ Technology Architecture ▪ Security Architecture Organisational Readiness Service Lifecycle Plan ▪ Planning Requirements ▪ Implementation Considerations ▪ Refresh Requirements ▪ Service Decommissioning Requirements Summary of Impact
Derivation of Deliverable	The Solution Overview is derived from the following: ▪ EUC Service Description (Service Requirements) ▪ Post Office Technical Reference Documentation
Allocated to	Supplier
Quality Criteria for Deliverable	▪ Delivered to the format specified ▪ Alignment to the PID ▪ Traceability to high level solution requirements
Quality Method	
People or skills required	**Reviewers** ▪ Post Office EUC Implementation Project Manager ▪ Post Office Service Design Lead ▪ Post Office Architecture Lead ▪ Post Office EUC Re-procurement Programme Manager ▪ Other suppliers (as required)

POL00337657

	Approval ▪ Post Office Programme representatives, dependent on the stakeholders identified in the PID For info to ▪ Stakeholders ▪ Team Members
First Draft Delivery Date for Deliverable	Within 20 working days of Project Notification
Planned Successful Approval Date for Deliverable	As per the Implementation

Table 27: *Solution Overview (SO) Product Description*

9.18 Implementation Milestones

The table below outlines the milestones that shall be required to be achieved to complete the implementation of EUC Services.

Payment Milestone	Implementation Milestone	Description
1	**1.1**	Start Up & Due Diligence
	1.2	Implementation Plan & PID Created & Approved By Post Office
2	**2.1**	Staff Transition TUPE to new Supplier- Branch (if required)
	2.2	Knowledge Transfer, Documented & Completed – Branch
	2.3	Service Management Work Instructions Created – Branch
	2.4	Operational Acceptance Certification – Branch
	2.5	EUC Service Implementation, Cutover & Go live – Branch
3	**3.1**	Staff Transition TUPE to new Supplier – Colleague (if required)
	3.2	Knowledge Transfer, Documented & Completed- Colleague
	3.3	Service Management Work Instructions Created – Colleague
	3.4	EUC Service Implementation, Cutover & Go live – Colleague
4	**4.1**	Close – End of Early Life Support & Project Closure

Table 28: *Implementation Milestones*

9.19 Implementation Schedule

The table below outlines a typical implementation schedule showing activities in a predicated sequence that will enable the end to end implementation of the Suppliers EUC Service.

	2021																			
	August					September					October					November				
Start Up & Due Diligence																				
High Level Plan, PID & RAID																				
Solution Overview																				
Security Management Plan																				
Test Strategy																				
Project Requirements Specification																				
BCDR Plan																				
Quality Plan																				
Deliverables Matrix Document																				
Level 4 Detailed Plan																				

POL00337657

Staff Transition TUPE																			
Knowledge Transfer																			
Service Management Work Instructions Created																			
Test Report																			
Detailed Cut Over Plan																			
Go live																			
Early Life Support																			
Operational Acceptance Certification																			
Project Closure Report																			
Implementation Complete																			

9.20 Acceptance Criteria

Each Milestone & deliverable shall have an Acceptance Criteria aligned to the Document Deliverables. Acceptance Criteria shall outline the method and steps taken to achieve or exceed the criteria. The types of Acceptance Criteria that shall be used include:

- Document Deliverables have been reviewed and approved based on meeting their quality criteria.
- Confirmation and compliance of delivered services meeting the Project Requirements.
- Evidence of testing being successful based on meeting or exceeding agreed test criteria.
- Operational processes, procedures and tooling in place that will support and manage the service.
- Agreement that early life support is in place and is suitably skilled and resource.
- Service operating procedures tested and in place.
- All hardware and assets are in place to deliver the service and are fully operational.
- All licenses and contracts with any third parties are in place.
- Any work in progress has been identified and a plan and owner has been agreed to complete to closure.

9.21 Testing

Project Test Strategy which forms part of the Documentable Deliverables shall be created by the EUC Supplier within 20 working days of project notification. The EUC Supplier shall agree to perform all testing to the standards set out in the Project Test Strategy. Within five working days of the completion of Testing, the Supplier shall provide Post Office with the completed Test Report which shall include:

- A synopsis of the Tests that were performed.
- Confirmation as to which successful test criteria was met.
- Confirmation as to which test criteria did not successful pass and an explanation from the EUC Supplier on the cause of the test not meeting the test criteria.
- Any tests that were not completed and an explanation from the EUC Supplier as to why they were not achieved.
- Should any Deliverables not meet its test criteria then the Supplier shall resolve the root cause of the issue and retest the Deliverable.

Schedule RM3804-A1 further outlines details of testing requirements and standards.

POL00337657

9.22 Change Freeze

The run up to Christmas is the busiest time of the year for Post Office. During this peak period, IT systems are key to delivering a good customer experience and to support this, Post Office implement a change freeze.

The change freeze is in place to protect Post Office during the peak period and to protect against the additional risks associated with change at this time of the year:

- Critical Business Period
- Public holidays in close succession
- Staff leave
- Reduced availability of public transport
- Increased use of applications, particularly those processing financial transactions
- The end of one year and the start of a new one

To support business goals and protect the most important & critical services the change freeze is typically phased, with an extended change freeze period for Branch related technologies and a shorter change freeze for Back Office and Colleague related services where there is no impact on Branch services.

For Branch Services, this change freeze is normally the last week prior to the end of November through to the first week of January.

For Back Office / Colleague this change freeze is normally mid-December through to the first week of January.

An example Change Freeze announcement for the Peak Christmas period 2020 is provided in **Appendix A – Doc-010-Change Freeze Example.**

Therefore, it would not be expected that the EUC Supplier would look to Implement Services during this period.

POL00337657

10. TRANSFORMATION

10.1 Transformation Overview

Transformation refers to in-scope projects which the EUC Supplier will deliver during agreed timescales within the EUC contractual milestones. Below are details of the in-scope project requirements.

An indication of potential future projects are provided in Section 11 Post Office Future Roadmap / Projects. Future projects beyond the in-scope requirements described in this section will be specified through Project Services – "Request for Quotation" process as defined in Section 6. If required, a change to the call of contract will be invoked through the RM3804 – Call Off TC v6 – Schedule 5: Variation Form.

10.2 Phases of Transformation Project

Each project will be structured against the following key phases of the project lifecycle and the EUC Supplier should base their plans accordingly:

- Phase 1 – Initiation
- Phase 2 – Design
- Phase 3 – Build, test & deliver
- Phase 4 – Acceptance

10.3 Project Governance

All projects in this Transformation section must comply with the appropriate requirement defined for Project Services as defined in Section 6 (e.g. governance and reporting requirements etc.)

10.4 Change Freeze

With reference to the previous section, 9.22 Change Freeze, related to Implementation, suppliers should note the normal Peak Period change freeze periods and plan implementation of projects around these restrictions.

An example Change Freeze announcement for the Peak Period 2020 is provided in **Appendix A – Doc-010-Change Freeze Example.**

10.5 Colleague Windows 10 Upgrade Project

10.5.1 Windows 10 Upgrade Overview

With reference to sections **3.3 Colleague Userbase Overview** and **4.5 Colleague Technologies** described above, the majority of the deployed devices in the Colleague estate utilise Windows 8.1 as an operating system with the remainder operating on a pilot Windows 10 build. These devices are predominantly out of warranty and end of service life.

The EUC Supplier will be required to adopt the Post Office Windows 10 build which has been created in the Win 10 Pilot and will have been further developers in the Post Office's Windows 10 Build Pilot and Delivery Project (see below). The EUC Supplier will then finalise this build to have full business application coverage.

POL00337657

The Windows 10 Build will need to support both of:

1. The existing legacy hardware within the estate.
2. New hardware which will be provisioned in stages throughout the contract (further details below).

The EUC Supplier will use the completed Windows 10 build to deploy to existing Colleague Devices (with the exception of a portion of device refreshes where a new device will also be deployed as detailed below).

The EUC Supplier will then fully support and manage the corporate Windows 10 build, utilising modern management technologies.

10.5.2 Post Office Windows 10 Build Pilot and Delivery Project

The Post Office has commenced an Autopilot Modern Management Windows 10 build pilot for the migration of all devices & apps from Windows 8.1 to Windows 10 in the Colleague estate. Currently there are 200 Windows 10 Surface Pro devices that are Azure AD joined and are enrolled within Microsoft Endpoint Manager to enable the functionality for Post Office to control the devices configuration and apply restrictions (See section 4.5.7 Windows 10 Design above for further details).

Following this pilot, the Post Office is due to commence a Windows 10 Build Pilot & Delivery Project which will develop the Windows 10 build so that it contains/ can provision approximately 80% of the required business applications.

This Windows 10 build will be used to provide 120 Disaster Recovery devices and further will be used in a break-fix roll out / new starter rollout of the Windows 10 build to approximately 300 replacement Colleague devices.

By the point of Service Commencement of the EUC Services contract, the supplier should assume the following status of Windows 10 rollout to the Post Office Colleague estate:

Device	Models	Numbers	Operating System
Tablet (Pilot)	Surface Pro 7 Pilot	200	Windows 10
Main Laptop	New Standard Laptop	300	Windows 10
Disaster Recovery Devices	New Standard Laptop	120	Windows 10

Table 29: *Assumed status of Windows 10 Roll Out at Service Commencement.*

The EUC Supplier should therefore assume the following devices will be in scope of the Windows 10 Upgrade Project (exact numbers to be confirmed during Windows 10 Upgrade Project Discovery stage, with plans / costs amended as required:

Device	Models	Numbers	Operating System
Main Desktops	M79 SFF	591	Windows 8.1
Additional Desktops	M79, M910, P510	8	Windows 8.1
Main Laptops	Thinkpad T440s	1359 (1659-300)	Windows 8.1
Additional Laptops	T440, T450, T450s, T460s, T540p, T560, T570	200	Windows 8.1
Total		**2158**	

Table 30: *Colleague Windows 10 Upgrade Scope*

10.5.3 Device Hardware Upgrade Provision

POL00337657

Due to financial profiling, a rolling upgrade of the Colleague legacy hardware will be completed over the term of the contract. This will be based on the following assumed volumes of devices made available for hardware upgrades:

Financial Year: April 2021 to March 2022 (FY21/22)	650
Financial Year: April 2022 to March 2023 (FY22/23)	650
Financial Year: April 2023 to March 2024 (FY23/24)	650
Financial Year: April 2024 to March 2025 (FY24/25)	650
Financial Year: April 2025 to March 2026 (FY25/26)	650
Total	3,250

Table 31: *Device Hardware Refresh Allocation*

The EUC supplier should note Hardware device purchase is out of scope of the Win 10 Upgrade Project and the EUC Services Contract. These devices will be purchased by Post Office via the CCS RM6060 Technology Products and Associated Services (TePAS) framework (or other Post Office approved route /framework). The EUC Supplier may be required to facilitate the transaction to purchase the required hardware via the TePAS/other route acting as the Post Office Agent for this purchasing route.

The Supplier should further note that **Post Office do not require options for 'Device as a Service' solutions.** The scope of the EUC Contract services requires the EUC Supplier to deliver the device management /managed device services only.

10.5.4 Windows 10 Build Software Licenses and Costs

Bidders should note that Windows 10 operating system and Post Office Windows 10 build software licenses and license costs are owned and purchased by Post Office and as such bidders do not need to include these costs in their Windows 10 Upgrade Project bid response.

POL00337657

10.5.5 Colleague Role Personas

Consumers of Colleague IT Services can be broadly separated into seven Personas;

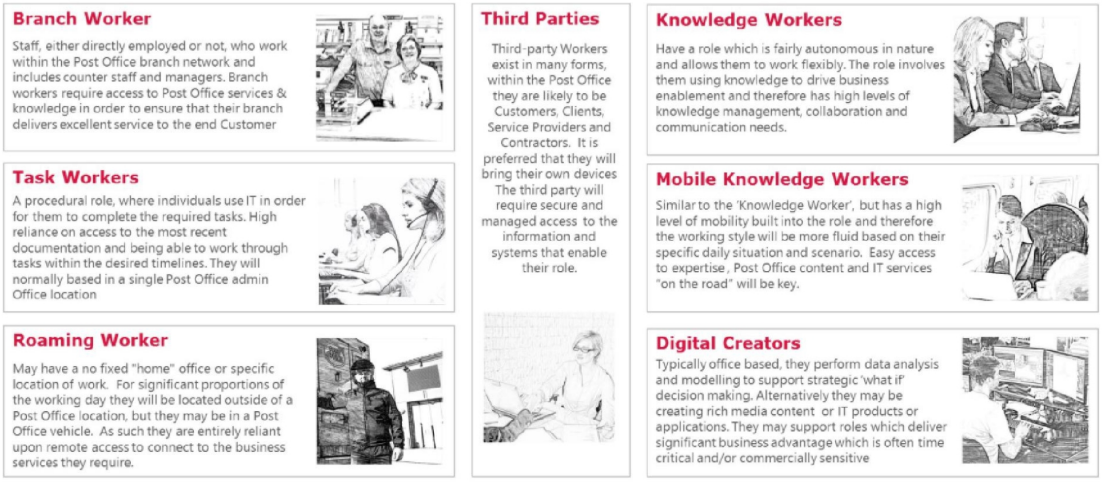


Figure 18: *Consumer types – Colleague IT services*

In terms of total numbers of each Persona, there are approximately:

- 990 Branch Workers
- 920 Knowledge Workers
- 880 Task Workers
- 380 Mobile Knowledge Workers
- 110 Roaming Workers
- 45 Digital Creators

10.5.6 Relationship with Shared Services Separation Project

The upgrade of the Colleague Win8.1 clients to Windows 10 is a key enabler of the approach for the Shared Services Separation Project (defined below). Moving to Windows 10 allows the Colleague clients to be managed via the Modern Management technologies, such as Win10 Autopilot, Microsoft Endpoint Manager (InTune), Azure AD etc.

To complete the full Shared Services Separation, the Colleague Windows 10 devices will operate in a Cloud management solution, where no dependencies on the legacy Shared Services components remain. For example, there may currently be application authentications which require a connection to the legacy Active Directory, or services/applications which require the Cisco VPN connectivity to operate. The Shared Services Separation project is tasked with removing these legacy dependencies.

To allow the Colleague estate to be upgraded to Windows 10 at the earliest opportunity, it is therefore acceptable for the Windows 10 Upgrade project design to rely on a 'hybrid' state where for example the Windows 10 devices use Hybrid Azure AD join, and some applications may require the Cisco VPN to operate.

As such suppliers may consider the Windows 10 Upgrade project to be a stepping-stone/ first stage towards Shared Services Separation.

10.5.7 Anticipated activities

POL00337657

The following activities are key anticipated activities for the Colleague Win 10 upgrade, these are provided to assist with defining the expected scope, plan and costs of the Colleague Windows 10 Upgrade project. Suppliers should include these tasks and in addition use their expertise to adjust these activities as required in forming the Win 10 Upgrade plan and activities as required in their response to the EUC Services tender.

Project Lifecycle Stage	Activity	Description
Initiation	Start-up	The EUC Supplier will complete the required start-up activities to launch the Win10 Upgrade project, engaging with the requisite stakeholders within Post Office.
	Discovery	The EUC Supplier will complete a discovery phase to ensure that the assumptions and base information they have built the plan and costs on are validated, and to gather any additional further details required.
	Win 10 Plan & PID	The EUC Supplier will create a Win10 Upgrade project plan with a full set of activities required by function (e.g. Architecture, Test etc) to allow the project to be comprehensively managed and monitored. The EUC Supplier will also create a Win10 Upgrade project PID (Project Initiation Document). The PID will include all of the planning components that address scope, budget, schedule, quality, configuration management, risks, issues and performance/qualify monitoring.
	Solution Overview (HLD)	The EUC Supplier will create a Solution Overview to present a common understanding of the solution to be delivered prior to entering the detailed Design phase of the Project.

POL00337657

Design	Application Inventory & Compatibility Assessment	The EUC Supplier will perform a Windows 10 compatibility assessment against in scope set of applications. This assessment will need to review the application dependencies on legacy technologies included in shared services and provide an option for migrating the identified legacy applications to Cloud equivalents, or delivering the Win10 upgrade using a hybrid model prior to the full separation from the Shared Services infrastructure components (e.g. Active Directory Hybrid Join, use of VPN to connect to legacy services etc). As part of this, the design for the existing Windows 10 Autopilot build should be reviewed and updated to meet the application integration requirements.
	Application Rationalisation	The EUC Supplier will work with Post Office IT and Post Office business representatives to rationalise the list of current applications to those required on the new Windows 10 build.
	Solution Design (LLD)	Update the build design with the IT, InfoSec and Business requirements. The updated design shall introduce a Windows service model that is focused on continually providing new capabilities and updates while maintaining a high level of hardware and software compatibility.
	Test Strategy & Plan	The EUC Supplier will create a Test Strategy and Plan for the Win10 Upgrade project, Pursuant to the requirements of RM3804-Alternative-and-additional-tc-v4, Call Off Schedule A1 Testing.
Build test & deliver	Application Migration	Migrate in-scope Windows 8.1 applications and services to Windows 10 Modern Management and use cloud native applications where possible.
	Build preparation	Integrate additional hardware devices into Autopilot deployment e.g. legacy devices such as T440 and newer laptop & desktop models.
	Testing and Operational Acceptance	The EUC Supplier will perform the agreed test strategy and plan for the Win10 Upgrade project, Pursuant to the requirements of RM3804-Alternative-and-additional-tc-v4, Call Off Schedule A1 Testing, including the provision of the requisite test certification for approval by Post Office.
	Deployment	The EUC Supplier will deliver the deployment of the Windows 10 build

POL00337657

		across all Colleague legacy devices as well as the portion of device upgrades available with the financial year restrictions described above. The supplier will coordinate the provision of new devices via the agreed Post Office hardware procurement route (e.g. CCS TePas framework).
Acceptance	Project Closure Report	On successful deployment of the Win10 upgrade project, the EUC Supplier will produce a Project Closure Report for review and approval by Post Office.

Table 32: *Windows 10 Project Anticipated Activities*

10.5.8 Milestones

Payment Milestone	Win 10 Upgrade Milestone	Description
5	**5.1**	Start Up
	5.2	Win 10 Plan & PID
6	**6.1**	Discovery
	6.2	Solution Overview
7	**7.1**	Application Remediation
	7.2	Colleague Win 10 build Operational Acceptance
8	**8.1**	25 % Estate Migrated to Windows 10
9	**9.1**	50 % Estate Migrated to Windows 10
10	**10.1**	75 % Estate Migrated to Windows 10
11	**11.1**	100 % Estate Migrated to Windows 10
12	**12.1**	Project Closure Report

Table 33: *Windows 10 Upgrade Project Milestones*

10.5.9 Timescales for the Windows10 Upgrade Project

The EUC Supplier will provide the detailed plan and timescales for the Windows 10 Upgrade project; however, the EUC Supplier should note the Post Office desire to achieve a successful early rollout of Windows 10 across the Colleague devices.

Deadline requirement: The supplier will ensure the Windows 10 Upgrade migration is complete no later than 12 months following completion of Implementation.

POL00337657

10.6 Shared Services Separation Project

10.6.1 Shared Services Project Overview

With reference to section 4.2 Shared Services, Shared Services refers to back-end infrastructure-based technologies and services that support both the Branch and Colleague estates. Shared Services infrastructure includes Microsoft Endpoint Manager (Intune), Active Directory and its associated technologies such as DNS and DHCP, SCCM and certificate services.

Currently, Shared Services are managed as a single unit of infrastructure that serves both the Branch and Colleague towers. This has previously caused several issues including the fact that changes to one tower can impact the other. To minimise this, the EUC Supplier will be required to work with Post Office to migrate the Colleague-related Shared Services to a new and modern management technology solution, where all devices and applications are managed and delivered through native cloud technologies, leaving the existing Shared Services for the management of Branch counters and devices.

10.6.2 Shared Services Separation Approach (Phases)

This migration of Shared Services is broken into 3 key phases described in the diagram below. Phase 1 is underway and will be complete prior to commencement of the EUC Services contract. Phase 2 is the required phase described in this in-scope project. Phase 3 is a potential future phase focused on the Branch-related Shared Services.

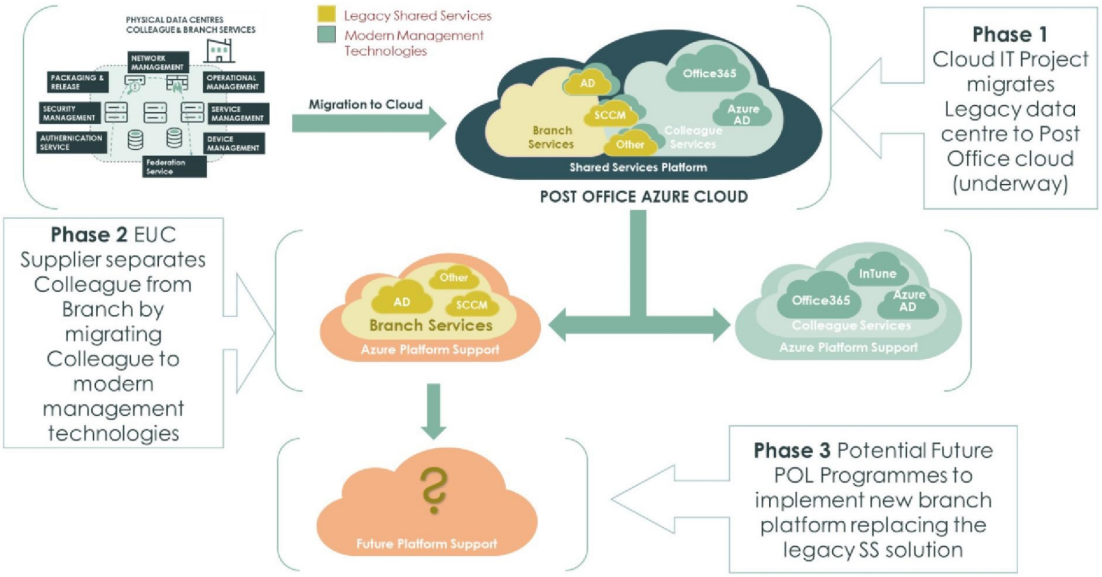


Figure 19: *Shared Services Approach Phases*

Key principles of this phased approach are as follows:

1. The current /legacy Shared Services will be fully hosted in the Post Office Azure Cloud prior to the commencement of the EUC Services contract.
2. The current EUC supplier will manage and support the Shared Services within the Post Office Azure cloud through to contract commencement of the new EUC Contract and completion of Implementation.
3. The EUC Supplier will then deliver the Shared Services Separation Project to migrate the Colleague-related Shared Services to Modern Management Technologies.

POL00337657

4. The migration of Colleague will be achieved through the upgrade of all Colleague devices to Windows 10 (See Windows 10 Upgrade Project) and the removal of any remaining dependencies on the legacy Shared Services infrastructure (e.g. any application dependencies on legacy Active Directory for authentication, where this will be moved to cloud-based / Azure AD authentication).
5. The approach of migrating Colleague away from the legacy Shared Services is required rather than an approach where current legacy Shared Services are 'duplicated' to affect the separation of Colleague and Branch as this is anticipated to represent significant and unnecessary 'sunk' costs.
6. The Branch services will remain on the legacy Shared Services infrastructure with minimal change.
7. Changes to the Branch environment, especially client configuration changes or updates must be minimised for the following reasons:
    a. Any risk of accidental outage to Branch services must be minimised and mitigated.
    b. Change expenditure on the Branch services / Shared Services infrastructure should be minimised since Phase 3 may result in a full deviation from the current technologies used (i.e. this would represent wasted expenditure).
8. Key 'house-keeping' activities to clean-up residual Colleague configurations, accounts, software packages etc from the remaining Legacy Shared Services used to support Branch will be completed to ensure a well-managed, secure and efficient environment.

10.6.3 Shared Services Components (current and target states)

The current shared services technologies are shown in the below figure.

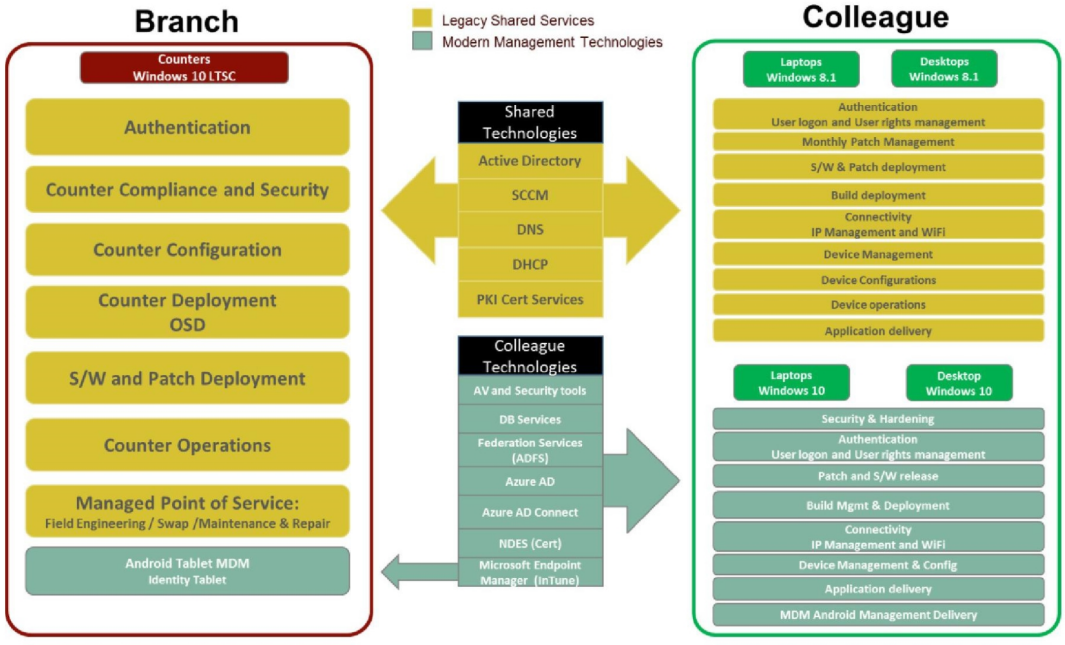


Figure 20: *Current State Shared Services Technology Components*

It should be noted there is currently a deployment of circa 800 Identity Tablets in the Branch estate which are dependent on the common Microsoft Endpoint Management (InTune) solution which is also used for the Pilot Win10 devices. For a full technical separation of the

POL00337657

two business areas, the EUC Supplier will be required to design the best (least impact) solution to provide an independent Branch solution for these Identity Tablets.

Through the phased approach described above, the Shared Services Separation project (and delivery of the Win10 Upgrade Project) will deliver the following high-level target management state:

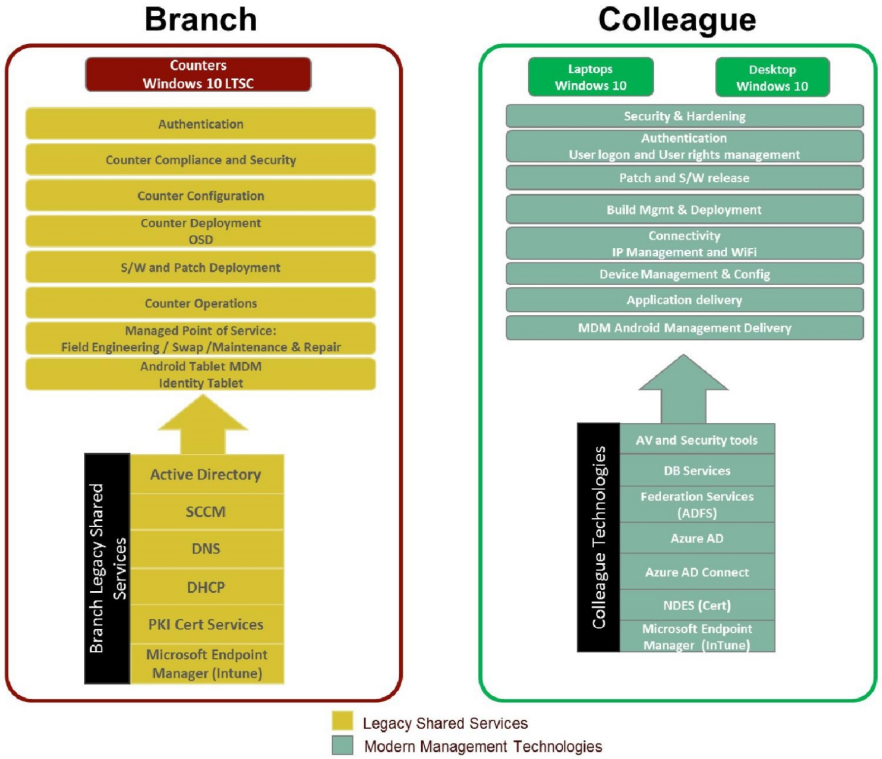


Figure 21: *Target State Branch Legacy Shared Services, and Colleague Modern Management Technology Components*

10.6.4 Relationship with Win10 Upgrade Project

As described in the Windows 10 Upgrade project, there is an anticipated relationship between the Windows 10 upgrade and the Shared Services Separation project. The upgrade of Colleague devices to Windows 10 allows the Colleague clients to be managed via the Modern Management technologies, such as Win10 Autopilot, Microsoft Endpoint Manager (InTune), Azure AD etc. This removes some dependencies on the legacy Shared Services, for example the use of SCCM for build and software/patch deployment is no longer required.

As described in the Windows 10 Upgrade Project section above, in order to complete the full Shared Services Separation, the Colleague Windows 10 devices will operate in a Cloud management solution, where no dependencies on the legacy Shared Services components remain. For example, there may currently be application authentications which require a connection to the legacy Active Directory, or services/applications which require the Cisco VPN connectivity to operate. The Shared Services Separation project is tasked with removing these legacy dependencies.

Suppliers should consider where there may be opportunities to combine the Windows 10 Upgrade project and Shared Services Separation projects activities and timelines, however the preference is that this does not materially impact the timely delivery of a Windows 10 upgrade to the Colleague devices at the earliest opportunity.

POL00337657

10.6.5 Anticipated activities

The following activities are key anticipated activities for the Shared Services Separation Project, these are provided to assist with defining the expected scope, plan and costs of the project. Suppliers should include these tasks and in addition use their expertise to adjust these activities as required in forming the Shared Services Separation plan and activities as required in their response to the EUC Services tender.

Project Lifecycle Stage	Activity	Description
Initiation	Start-up	The EUC Supplier will complete the required start-up activities to launch the Shared Service Separation project, engaging with the requisite stakeholders within Post Office.
	Discovery	The EUC Supplier will complete a discovery phase to ensure that the assumptions and base information they have built the plan and costs on are validated, and to gather any additional further details required.
	Shared Services Separation Plan & PID	The EUC Supplier will create a Shared Services Separation project plan with a full set of activities required by function (e.g. Architecture, Test etc) to allow the project to be comprehensively managed and monitored. The EUC Supplier will also create a Shared Services Separation project PID (Project Initiation Document). The PID will include all of the planning components that address scope, budget, schedule, quality, configuration management, risks, issues and performance/qualify monitoring.
	Solution Overview (HLD)	The EUC Supplier will create a Solution Overview to present a common understanding of the solution to be delivered prior to entering the detailed Design phase of the Project.
Design	Infrastructure Assessment	The EUC Supplier will complete a detailed infrastructure assessment to ascertain dependencies and integrations of the Colleague Windows 10 applications and the legacy Shared Services solution (note relationship with Win10 Upgrade project '*Application Inventory & Compatibility Assessment*' activity).
	Solution Design (LLD)	Update the build design with the detailed IT, InfoSec and Business requirements.
	Test Strategy & Plan	The EUC Supplier will create a Test Strategy and Plan for the Shared Services Separation project, Pursuant to the

POL00337657

		requirements of RM3804-Alternative-and-additional-tc-v4, Call Off Schedule A1 Testing. The Test Strategy and Plan will pay particular attention to measures to minimise any risk of service outage in the Branch estate as a result of Shared Service separation activities.
Build test & deliver	Application integration migration	The EUC Supplier will deliver application changes and cloud-migrations as necessary to remove Colleague integration/dependencies on the legacy Shared Service infrastructure.
	Testing and Operational Acceptance	The EUC Supplier will perform the agreed test strategy and plan for the Shared Services Separation project, Pursuant to the requirements of RM3804-Alternative-and-additional-tc-v4, Call Off Schedule A1 Testing, including the provision of the requisite test certification for approval by Post Office.
	Legacy Shared Services housekeeping	The EUC Supplier will complete required housekeeping activities to remove legacy Colleague configurations, accounts, software packages etc from the Legacy Shared Services infrastructure, leaving only the Branch aspects for ongoing management and maintenance.
Acceptance	Project Closure Report	On successful deployment of the Shared Services Separation project, the EUC Supplier will produce a Project Closure Report for review and approval by Post Office.

Table 34: *Shared Services Separation Project Anticipated Activities*

10.6.6 Milestones

Payment Milestone	Shared Services Milestone	Description
13	**13.1**	Start Up
14	**14.1**	Discovery
	14.2	Shared Services Plan & PID
15	**15.1**	High Level Design (HLD)
	15.2	Low Level Design (LLD)
16	**16.1**	Colleague Infrastructure Services Cutover
17	**17.1**	Project Closure Report

Table 35: *Shared Services Separation Project Milestones*

10.6.7 Timescales for the Shared Services Separation Project

The EUC Supplier will provide the detailed plan and timescales for the Shared Services Separation project; however, the supplier should note the Post Office desire to achieve a successful early separation of the Colleague management services (utilising modern management tools).

POL00337657

Deadline requirement: The supplier will ensure the Shared Services Separation is complete no later than 18 months following completion of Implementation.

10.7 Analytics Project (Exercisable Option)

Post Office Limited would like suppliers to propose a project which will provide an Analytics solution providing real-time Analytics for all in-scope End User Devices to gather and monitor endpoint activity, network connectivity, and end-user experience.

This is project is an Exercisable Option which will be initiated at Post Office Limited's sole discretion during the EUC Services contract.

If this project is initiated, the requirements detailed below in section 10.8.2 will be incorporated into the Service Specification under Monitoring and Reporting (section 6 - Service Specification)

10.7.1 Analytics Project Overview

The Post Office Limited would like to gain visibility across the digital EUC environments and explore strategies that will eliminate digital friction and power productivity for the remote, hybrid, or on-site workforce.

The scope of this project is the Colleague estate only.

Via this Analytics Project, Post Office Limited would like the EUC Supplier to implement a digital experience management solution, suitable for the Colleague environment, that provides data-driven analytics and insight for continuous improvement and aids easy identification of which resources are causing poor service quality.

The solution should help improve end-user experience and productivity through expanded IT visibility, end-user experience scoring, self-help engagement, persona-based segmenting, and other insights.

The solution should also take a more proactive approach to IT support by harnessing artificial intelligence capabilities for quicker remediation, ITSM optimisation, automation, and enabling the Post Office Service Desk – first line support.

The EUC Supplier will be required to implement an Analytics solution which can achieve the following requirements:

POL00337657

Req ID	Requirement Description
EUC-AN-01	The Supplier shall, enable the Customer with a real-time analytics solution suitable for all in scope End User Devices to gather and monitor endpoint activity, network connectivity, and end-user experience as the basis for automating the remediation of service issues. The solution should have the following capabilities (but not limited to):- (a) capture Real-time User/digital Experience Telemetry (scoring etc.); (b) capture Remote access and remote working experience; (c) provide visibility of Network speed/latency and other network QOS related issues; (d) monitor and capture Application usage and metering; (f) monitor and capture application and system errors and faults; (g) provide customised dashboards based on the Customer's requirements; (h) monitor and capture device performance; (i) provide event level visibility (Real-time); and (j) integrate into Customer's ITSM solution and provide automated remediation where applicable.
EUC-AN-02	The Supplier shall, use the analytics solution to provide Customer with regular reports on End User experience and devices.
EUC-AN-03	The Supplier shall, use the analytics solution to provide proactive support to the Customer to continuously identify and implement technical solutions to common IT business challenges.
EUC-AN-04	The Supplier shall, use the analytics solution to deliver evidence-based decision making to help with continuous improvement and problem/incident management activities, which may include other solutions delivered by other Suppliers.
EUC-AN-05	The Supplier shall, provide the Customer with read access to the analytics solution and the ability to generate reports.
EUC-AN-06	The Supplier shall, work with the Customer to create dashboards/reports and MI data as required, including project, Security and Business as Usual work.

Table 36: *Analytics Project Service Requirements*

10.7.2 Anticipated activities

The following activities are key anticipated activities for the Analytics project, these are provided to assist with defining the expected scope, plan and costs of the project. The supplier should include these tasks and in addition use their expertise to adjust these activities as required in forming plan and activities as required in their response to the EUC Services tender.

Project Lifecycle Stage	Activity	Description
Initiation	Start-up	The EUC Supplier will complete the required start-up activities to launch the Analytics project, engaging with the requisite stakeholders within Post Office.
	Discovery	The EUC Supplier will complete a discovery phase to ensure that the assumptions and base information they have built the plan and costs on are

POL00337657

		validated, and to gather any additional further details required.
	Analytics Project Plan & PID	The EUC Supplier will create an Analytics Project plan with a full set of activities required by function (e.g. Architecture, Test etc) to allow the project to be comprehensively managed and monitored. The EUC Supplier will also create an Analytics Project Upgrade project PID (Project Initiation Document). The PID will include all of the planning components that address scope, budget, schedule, quality, configuration management, risks, issues and performance/qualify monitoring.
	Solution Overview (HLD)	The EUC Supplier will create a Solution Overview to present a common understanding of the solution to be delivered prior to entering the detailed Design phase of the Project.
Design	Solution Design (LLD)	Update the build design with the IT, InfoSec and Business requirements. The LLD will provide all required technical and support design details to allow approval to move to the build and delivery phase.
	Test Strategy & Plan	The EUC Supplier will create a Test Strategy and Plan for the Analytics Project, Pursuant to the requirements of RM3804-Alternative-and-additional-tc-v4, Call Off Schedule A1 Testing.
Build test & deliver	Build and Pilot	The designed solution will be built and deployed to a pilot user/system base where testing and confirmation of the solution can be completed.
	Deployment	The EUC Supplier will deliver the deployment of the Analytics Project solution, in-line with the agreed plan and schedule.

POL00337657

	Testing and Operational Acceptance	The EUC Supplier will perform the agreed test strategy and plan for the Analytics Project, Pursuant to the requirements of RM3804-Alternative-and-additional-tc-v4, Call Off Schedule A1 Testing, including the provision of the requisite test certification for approval by Post Office.
Acceptance	Project Closure Report	On successful deployment of the Analytics Project, the EUC Supplier will produce a Project Closure Report for review and approval by Post Office.

Table 37: *Analytics Project Anticipated Activities*

10.7.3 Analytics Project Software / License Costs

Where additional software / licenses are required, Bidders should include any costs associated with software / licenses for the proposed solution as an uplift to the service charges in the relevant section of the further Competition Attachment 3 EUC Financial Evaluation Model. For clarity, this solution should be delivered as a managed service by the EUC Supplier.

10.7.4 Milestones

Payment Milestone	Analytics Project Milestone	Description
Opt 1	**Opt 1.1**	Analytics Project Plan & PID
	Opt 1.2	Solution Overview (HLD)
Opt 2	**Opt 2.1**	Solution Design (LLD)
	Opt 2.2	Test Strategy & Plan
Opt 3	**Opt 3.1**	Build & Pilot
	Opt 3.2	Deployment & Operational Acceptance
Opt 4	**Opt 4.1**	Project Closure Report

Table 38: *Analytics Exercisable Option Project Milestones*

10.8 Remote Device Management (Exercisable Option)

Post Office Limited would like suppliers to propose a project which will provide a Remote Device Management solution providing the process(es) and system(s) to enable support functions to access end point systems (Colleague Laptops/Desktops and Branch Point of Sale devices) and perform resolution and maintenance activities.

This project is an Exercisable Option which will be initiated at Post Office Limited's sole discretion during the EUC Services contract.

If this project is initiated, the requirements detailed below in section 10.8.2 will be incorporated into the Service Specification under Service Operations (section 6 - Service Specification)

POL00337657

10.8.1 Remote Device Management Project Overview

Colleague Estate:
The Post Office Limited currently uses Microsoft SCCM in the Colleague environment to provide IT support teams and administrators the capabilities to remotely control end-user devices for troubleshooting. Owing to the SCCM's requirements for corporate network connectivity, the support teams are currently unable to resolve issues relating to connectivity and remote access.

To address the above, the EUC Supplier will be required to implement a Remote Device Management solution for the Colleague environment, providing the process(es) and system(s) to enable support functions to connect to and control End User devices from a remote location via an internal network or the internet to resolve technical issues and automate routine tasks.

Branch Estate:
Post Office currently does not have any remote desktop control capabilities in the Branch environment and as a result, the support teams are unable to perform fixes which require this type of solution remotely.

Within this project, the EUC supplier will be required to implement an audited process and use Microsoft Windows' native remote file and registry access capabilities for applying manual fixes on Post Office Windows 10 LTSB Branch counters. It is important to mention that full remote view and desktop takeover on Branch counters is not permitted and therefore only file and registry access should be considered as part of the Branch Remote Device Management solution.

The audited process mandates that the solution shall provide prominent notice and obtain consent from the Branch user before a remote session begins. Also, the process should record the name of the support engineer, the work that has been completed and the duration of the remote connection.

10.8.2 Remote Device Management Requirements

The solution should deliver the following requirements:

Req ID	Requirement Description
EUC-RSM-01	The Supplier shall, ensure that Supplier support agents have the ability to remotely access an End Users Device, including Branch counters, and resolve incidents whilst adhering to the Customer's Information Security Standards.
EUC-RSM-02	The Supplier shall, ensure IT Security have the ability to remote access EUC devices using appropriate controls for the investigation of High Severity Security Threats to: (a) extract critical analytic logs; (b) isolate devices from the network, which includes automation tool device takeover and isolation, during business hours and out of hours.
EUC-RSM-03	The Supplier shall, provide remote support capabilities as a default to analyse, diagnose or fix Incidents to the maximum possible extent prior to or instead of a site visit.
EUC-RSM-04	The Supplier shall, where applicable and practical, facilitate video calls with End Users to diagnose issues & avoid site visits.

POL00337657

EUC-RSM-05	The Supplier shall, where possible, integrate all remote systems management tools with the ITSM systems to allow first line fix and remediation.
EUC-RSM-06	The Supplier shall, implement, use and provide access to the Customer, tools that allow for automated and remote systems management and monitoring of the equipment (which, for the avoidance of doubt, includes Infrastructure) and software.
EUC-RSM-07	The Supplier shall, ensure that any remote monitoring and takeover activities are reported in real time of PAM via SIEM or ITSM integration, tracked and audited, as agreed with the Customer and in line with Security policies and processes.
EUC-RSM-08	The Supplier shall, log any changes which may have been made to applications or data on branch counter, as agreed with the Customer.

Table 39: *Remote Device Management Project Service Requirements*

10.8.3 Anticipated activities

The following activities are key anticipated activities for the Remote Device Management project, these are provided to assist with defining the expected scope, plan and costs of the project. The supplier should include these tasks and in addition use their expertise to adjust these activities as required in forming plan and activities as required in their response to the EUC Services tender.

Project Lifecycle Stage	Activity	Description
Initiation	Start-up	The EUC Supplier will complete the required start-up activities to launch the Remote Device Management Project, engaging with the requisite stakeholders within Post Office.
	Discovery	The EUC Supplier will complete a discovery phase to ensure that the assumptions and base information they have built the plan and costs on are validated, and to gather any additional further details required.
	Remote Desktop Management Project Plan & PID	The EUC Supplier will create a Remote Device Management Project plan with a full set of activities required by function (e.g. Architecture, Test etc) to allow the project to be comprehensively managed and monitored. The EUC Supplier will also create a Remote Device Management Project Upgrade project PID (Project Initiation Document). The PID will include all of the planning components that address scope, budget, schedule, quality, configuration management, risks, issues and performance/qualify monitoring.
	Solution Overview (HLD)	The EUC Supplier will create a Solution Overview to present a common

POL00337657

		understanding of the solution to be delivered prior to entering the detailed Design phase of the Project.
Design	Solution Design (LLD)	Update the build design with the IT, InfoSec and Business requirements. The LLD will provide all required technical and support design details to allow approval to move to the build and delivery phase.
	Test Strategy & Plan	The EUC Supplier will create a Test Strategy and Plan for the Remote Device Management Project, Pursuant to the requirements of RM3804-Alternative-and-additional-tc-v4, Call Off Schedule A1 Testing.
Build test & deliver	Build and Pilot	The designed solution will be built and deployed to a pilot user/system base where testing and confirmation of the solution can be completed.
	Deployment	The EUC Supplier will deliver the deployment of the Remote Device Management Project solution, in-line with the agreed plan and schedule.
	Testing and Operational Acceptance	The EUC Supplier will perform the agreed test strategy and plan for the Remote Device Management Project, Pursuant to the requirements of RM3804-Alternative-and-additional-tc-v4, Call Off Schedule A1 Testing, including the provision of the requisite test certification for approval by Post Office.
Acceptance	Project Closure Report	On successful deployment of the Remote Device Management Project, the EUC Supplier will produce a Project Closure Report for review and approval by Post Office.

Table 40: *Remote Device Management Project Anticipated Activities*

10.8.4 Remote Device Management Software / License Costs

Where additional software / licenses are required, Bidders should include any costs associated with software / licenses for the proposed solution as an uplift to the service charges in the relevant section of the further Competition Attachment 3 EUC Financial Evaluation Model. For clarity, this solution should be delivered as a managed service by the EUC Supplier.

10.8.5 Milestones

Payment Milestone	RSM Project Milestone	Description
Opt 5	**Opt 5.1**	Remote Device Management Project Plan & PID
	Opt 5.2	Solution Overview (HLD)

POL00337657

Opt 6	**Opt 6.1**	Solution Design (LLD)
	Opt 6.2	Test Strategy & Plan
Opt 7	**Opt 7.1**	Build & Pilot
	Opt 7.2	Deployment & Operational Acceptance
Opt 8	**Opt 8.1**	Project Closure Report

Table 41: *Remote Device Management Exercisable Option Project Milestones*

POL00337657

11. POST OFFICE FUTURE ROADMAP / PROJECTS

11.1 Post Office Future Roadmap / Projects Overview

This section describes the potential future strategic projects where Post Office may require the EUC Supplier's support. These projects do not form part of the scope of the EUC contract at this stage but are provided for information to the EUC supplier. Any engagement for involvement in these projects will be via the EUC Project Services Request for Quotation/Small Projects process or may be subject to further procurement competition as appropriate.

11.2 Strategic Platform Modernisation

Strategic Platform Modernisation (SPM) is a major Branch change initiative which aims to simplify Branch devices and peripherals. SPM is to provide an entire re-platforming of Branches within the next two or three years, alongside development of a new approach to the Branch application.

SPM is considering a move to non-Microsoft platforms such as Linux or Android based platforms. Additionally, the SPM programme aims to address:

- A reduction in the till physical size.
- Network bandwidth optimisation with regards to patching.
- Address build complexity.
- Improve monitoring and security scanning of branch equipment.
- Increased use of branch Wi-Fi.
- A standardisation of peripherals and ports.
- Branch enablement in terms of the ability for branches to self-serve.
- Increase the efficiency with regards to maintaining spare parts.
- Potentially provide new shared services back-end infrastructure cloud hosting arrangements to suit a Linux/ Android platform, potentially with AWS.

The implication of SPM to the EUC supplier is that there may be a requirement to support a different set of Branch technologies in the future, including devices and platforms.

The supplier will need to be able to work with Post Office and facilitate this transformation, while providing BAU operations, and providing products and services that are agnostic to the change where possible in order minimise the change impact.

There is therefore a need for the supplier to have the flexibility to adapt to this change which includes the ability to provide the required changes to component support teams.

11.3 Microsoft 365 E5

Post Office anticipates upgrading Microsoft E3 to E5 licenses and replacing legacy technologies with the E5 equivalents.

For the avoidance of doubt, Post Office does NOT require Suppliers to cost and plan implementation of these services at this time, but Suppliers should anticipate needing to move to these technologies for the delivery of the Services during the Period of the Agreement.

Microsoft 365 E5 combines best-in-class productivity apps with advanced security, compliance, voice and analytical capabilities. Post Office is likely to undertake the following implementations in-line with E5 technology:

POL00337657

- Replacing Mimecast and Ironscales with Office 365 ATP
- Implementing Office 365 Advanced Compliance
- Implementing Azure ATP
- Implementing Identity Protection and Privileged Identity Management (PIM)
- Replacing SEP with Microsoft Defender ATP

11.4 CviT (Cash & Valuables in transit) Drivers PDA Replacement

Due to the nature of the CviT use cases and health and safety considerations, Post Office intends to further investigate the options for completing the pilot (mentioned earlier) of the new Android devices and rolling out a full production solution.

The new Android devices will need to be enterprise ready and managed by the existing Windows 10 Modern Management Platform e.g. Microsoft Endpoint Manager. These devices will be fully managed for CviT drivers where all device access will be heavily customised, and policies applied to restrict non approved changes e.g. application installation and device setting changes. Additionally, internet access will be heavily restricted based on security groups.

POL00337657

12. GOVERNANCE

The Supplier shall participate in a governance process which involves a hierarchy of governance meetings, between the Supplier and Post Office, and feed upwards in the meeting hierarchy. The following provides a summary of the required governance forums.

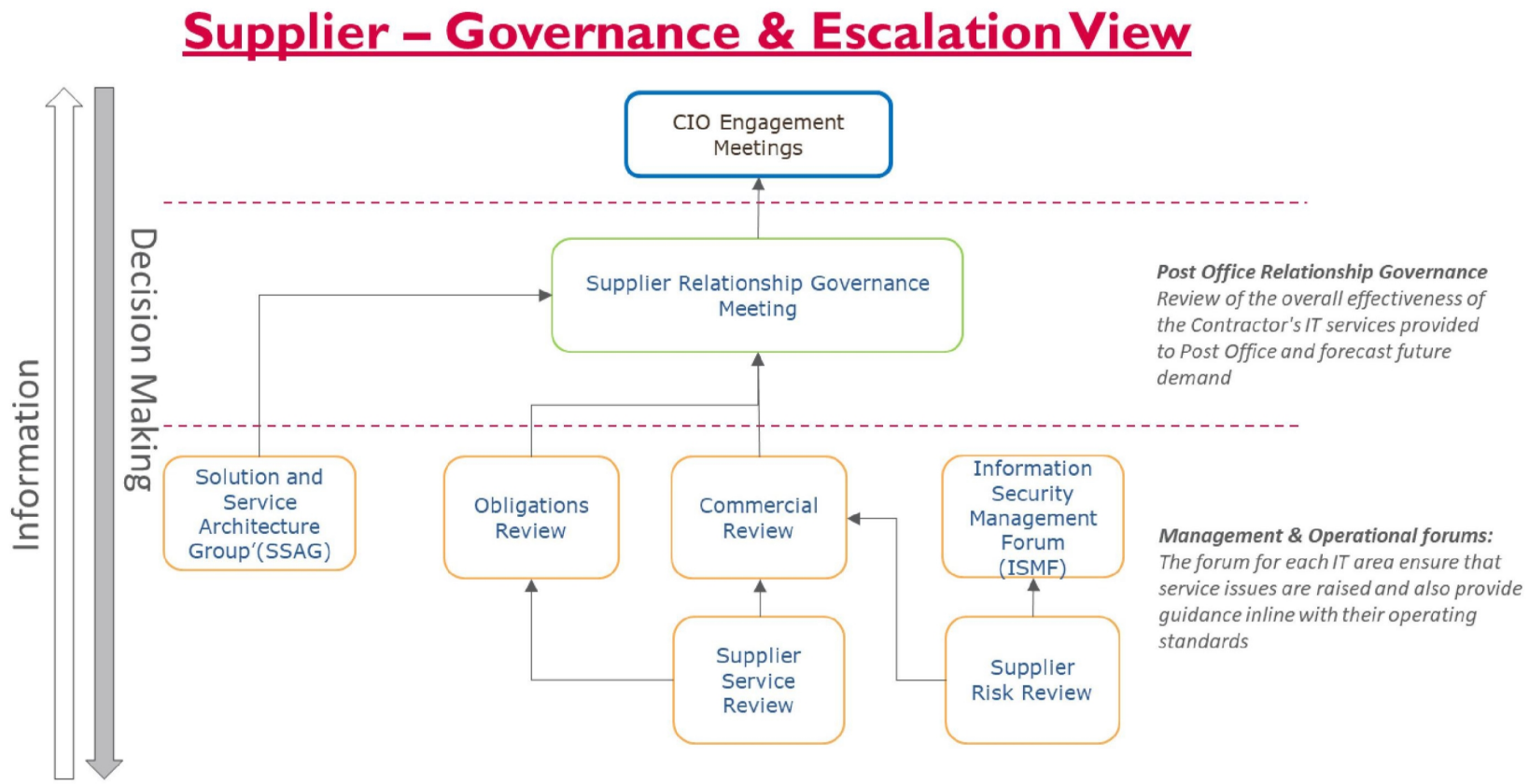


Figure 22: *Overview of Post Office Governance Forum*

POL00337657

12.1 Summary of Service Specification Governance / Meeting Requirements

The following provides a summary for convenience of the meeting requirements defined in Section 6 Service Specification:

Service Area	Reference	Meeting	Frequency
Cloud Platform Management	EUC-CPM-18	Management meeting to report on in-scope cloud hosted resources	Monthly
Field Engineer Services	EUC-FES-04	Monthly service review management report/dashboard and meeting review	Monthly
Configuration Management	EUC-CONM-07	CMDB review and performance meeting	Monthly
Financial and Contractual Management	EUC-FCM-13	Financial review meeting	Monthly
	EUC-FCM-14	Contractual review meeting	Monthly
Risk and Compliance	EUC-RC-08	Risks review meeting	Monthly
Service Management	EUC-SM-01	Daily stand up service reviews	Daily
		Weekly service line operational meetings	Weekly
		Monthly service review to cover all aspects of contracted services	Monthly
		Ad-hoc operational meetings e.g. Major Incident Review	Ad-hoc
		Quarterly Service Strategy review meeting	Quarterly
Incident Management	EUC-IM-09	Cross Functional/Supplier meetings to diagnose escalated Incidents (including Major Incidents)	Ah-Hoc / as required
Service Operations Change Management	EUC-SOCM-04	Customer's Change Advisory Board (CAB) meetings in respect of Significant and Major Change types.	Twice Weekly
IT Service Continuity Management	EUC-ITSCM-11	Post-disaster meeting with the Customer (as soon as reasonably possible)	As required
Project Change Management	EUC-PCM-14	Project Portfolio reviews	Monthly
	EUC-PCM-15	Ad-hoc Project Portfolio reviews, invoked by monthly portfolio reviews.	Ad-hoc
	EUC-PCM-21	Project Board Meetings	As required
Operational Business Change (OBC)	EUC-OBC-09	OBC planning meetings	Monthly
Request to Quote (RTQ)	EUC-RTQ-05	RTQ review meetings to assess and accept RTQ into the supplier process.	Twice Weekly
Availability Management	EUC-AVM-10	Availability Management meeting	Monthly

POL00337657

Capacity Management	EUC-CM-09	Capacity Management Meeting	Monthly
Event Management	EUC-EM-07	Event Management - to determine response selection for cross-functional Events.	As required

Table 42: *Summary of Service Specification Meeting Requirements*

POL00337657

13. APPENDIX A – LIST OF DOCUMENTS

The following documents are referenced throughout the Service Specification Document and are provided as attachments.

Ref No.	Referenced Document Name	Process and Policy Document Name
PP-001	Cyber Security Policy and Processes	PP-001-Cyber Security Policy and Standards zip
PP-001a	Asset Management Standards	PP-001-Cyber Security Policy and Standards zip
PP-001b	Access Control Standards	PP-001-Cyber Security Policy and Standards zip
PP-001c	Acceptable Usage Standards	PP-001-Cyber Security Policy and Standards zip
PP-001d	Cyber and Information Security Policy	PP-001-Cyber Security Policy and Standards zip
PP-001e	Cyber and Information Security Standard	PP-001-Cyber Security Policy and Standards zip
PP-001f	Document Retention & Disposal Policy	PP-001-Cyber Security Policy and Standards zip
PP-001g	Encryption Standards	PP-001-Cyber Security Policy and Standards zip
PP-001h	Information Classification Standards	PP-001-Cyber Security Policy and Standards zip
PP-001i	Network Security Guidelines	PP-001-Cyber Security Policy and Standards zip
PP-001j	Network Security Standard	PP-001-Cyber Security Policy and Standards zip
PP-001k	PED Tamper Monitoring & Skimming Prevention Guideline	PP-001-Cyber Security Policy and Standards zip
PP-001l	Platform Security Guidelines	PP-001-Cyber Security Policy and Standards zip
PP-001m	Platform Security Standards	PP-001-Cyber Security Policy and Standards zip
PP-001n	SDLT Guidelines	PP-001-Cyber Security Policy and Standards zip
PP-001o	SDLT Standards	PP-001-Cyber Security Policy and Standards zip
PP-002	Architecture Governance Framework	PP-002-Architecture Governance V3.0
PP-003	IT Service Continuity Policies and Processes	PP-003- IT DR Policy V1.4 (2019 Policy Template v1.2) docx
PP-004	IT Change Management Policies	PP-004- IT Change Management Policy v1.0 docx
PP-005	IT Change management Process	PP-005- CM-PRO-IT Change Management Process V2.2 docx
PP-006	IT Major Incident Management Process v5 pdf	PP-006- IT Major Incident Management Process v5 pdf
PP-007	POL Vetting Policy Postmasters Assistants pdf	PP-007-POL Vetting Policy Postmasters Assistants pdf

POL00337657

PP-008	Vetting Policy Employees	PP-008-Vetting Policy Employees_v.2.4_February 2021pdf
PP-009	POL Incident Management Operations Manual	PP-009-POL_Incident_Management_Operations__Manual v0.2 doc
PP-010	Quality Standards and Change Excellence Framework	PP-010- CEF ExtractCEF Extract zip
PP-010a	CEF Mandated Artefacts Relationships	CEF Mandated Artefacts Relationships
PP-010b	SPO advice on completing CEF templates	SPO advice on completing CEF templates
PP-010c	7 critical success factors	7 critical success factors
PP-010d	Agile Value Stack	Agile Value Stack
PP-010e	Benefits Management Workbook	BENEFITS MGMNT WRKBK PRJname PRJcode
PP-010f	Benefits Handover Certificate	BENEFITS TRF CERT PRJName PRJcode No X
PP-010g	Business Readiness Assurance Process	BRA Process ICONS
PP-010h	Business Readiness Assurance Template	BRA TEMPLATE PRJname PRJcode
PP-010i	Agile Business Case Template	BUSINESS CASE AGILE PRJname PRJcode
PP-010j	Waterfall Business Case Template	BUSINESS CASE WATERFALL PRJname PRJcode
PP-010k	Business Case Model Template	BUSINESS CASE MODEL PRJname PRJcode
PP-010l	Business Requirements Template	BUSINESS REQUIREMENTS PRJname PRJcode
PP-010m	Business Solution Design Template	BUSINESS SOLUTION DESIGN PRJname PRRJcode
PP-010n	Change Excellence Framework Process Flow	CE Framework ICONS
PP-010o	Communication Brief Template	COMMS BRIEF PRJname PRJcode version x
PP-010p	Document Deliverables Tracker	Document Deliverables Tracker
PP-010q	Gating Forum Template	GATING FORUM SUMMARY PRJname PRJcode
PP-010r	WBS request form	MD-WBS 1 - Masterdata WBS request
PP-010s	Programme Increment Funding Drawdown template	PI FUNDING DRAWDOWN REQ PRJname PRJcode
PP-010t	Project Initiation Document template	PID PRJname PRJcode
PP-010u	Project Change Request Template	PROJECT CHANGE REQUEST PRJname PRJcode Number X version y
PP-010v	Prove Plan template	PROVE PLAN
PP-010w	Request to Close Checklist	REQUEST TO CLOSE CHECKLIST PRJname PRJcode version x
PP-010x	Request to Close Report	REQUEST TO CLOSE REPORT PRJname PRJcode
PP-010y	Template Library overview	Template Library overview

POL00337657

PP-011	Release Management Policies and Processes	PP-011-POL Release Management Strategy docx.
PP-012	Service Transition Management Policies and Processes	PP-012-Service Design and Transition Policy v2 5 docx
Ref No.	Referenced Document Name	Document Name
Ref Doc-001	Service Request and Incident Metrics Document	Ref Doc-001-Service Requests & Incident Metrics Document docx
Ref Doc-002	Services Schedule 7.1 Annex	Ref Doc-002- Services Schedule 7.1 Annex.xlsx
Ref Doc-003	CC Service Management Guide for POL Redacted	Ref Doc-003-CC Service Management Guide for POL Redacted. Pdf
Ref Doc-004	POL Device Software	Ref Doc-004-POL Device Software xlsx
Ref Doc- 005	Software Document	Ref Doc- 005-Software Document.docx
Ref Doc-006	Service Catalogue v2	Ref Doc-006-Service Catalogue v2.xlsx
Ref Doc- 007	Colleague and Branch Locations	Ref Doc- 007-Branch and Colleague Locations xlsx
Ref Doc-008	Post Office OBC Process Doc	Ref Doc-008-OBC process doc_v0 5_UpdatedJan 2020 (7) (003) docx
Ref Doc-009	EUC ServiceNow Supplier Onboarding Guide	Ref Doc-009- EUC Service ServiceNow Supplier Onboarding Guide - v0.03 (003) docx
Ref Doc-010	Change Freeze Example	Ref Doc-010 – Change Freeze Example.docx
Ref Doc-011	Tupe List v1 (password protected)	Ref Doc-011-Tupe List v1.xlsx
Ref Doc-012	EUC Service Level Agreement MASTER	Ref Doc-012-EUC Service Level Agreement MASTER v1.0

Table 43: *List of Reference Documents*