POL00038770

BTTP / 10.11 Enhanced User Management

Business Solution Design

Governance

Presented to:	SUF 25.08.2016	**Date of Approval:**	
Outcome:	Recommended option accepted. Action now with SD team.		
Outcome Conditions:			

POL00038770

Contents

POL00038770

POL00038770

Management Summary

1.1. Business Problem

User Management describes the functionality that determines who is authenticated to use the Horizon system and what they can use the system for. In terms of Horizon today, there are nine different User Roles ranging from a Branch User to an External Auditor.

This document illustrates the processes related to management of a system User, from the initial registration and set up, through to any amendments and changes once the User is enlivened and through to the end point for a User when they are archived from the system, see Appendix D for the detailed AS IS process maps.

Access control defines the attribute which can be assigned to a User which determines what the system functions a User can access and action. This manifests itself in the defining of User Roles which are essentially default groupings of attributes determining the system functions which are accessible to a User.

The current processes lack control and an audit trail. Users are not restricted to the location and number of terminals they can log on to and crucially, there are no unique user ID's. This in turn makes it difficult to prove who has actually been operating the system at a given time and in case of fraudulent activity this makes proof of guilt or ownership of culpability difficult to prove.

Project Sparrow produced a number of improvement opportunities which relate to User Management which are detailed in section 2.2.2 below.

1.2. Drivers for Change

The present user management solution does not provide the necessary controls over who can access and transact on the Horizon system, thereby exposing the business to regulatory, financial and reputational damage. The business needs to be able to prove that staff are fully trained and compliant and that the business is meeting legal and regulatory obligations to both Clients and Authorities such as the International Civil Aviation Authority (ICAO), the Information Commissioner's Office (ICO) and the Financial Conduct Authority (FCA). In addition, the business must be able to protect the agreement it has with Royal Mail by proving we are compliant with the Mail Integrity Code of Practice.

1.3. Summary of Findings

The summary of key findings is as follows:

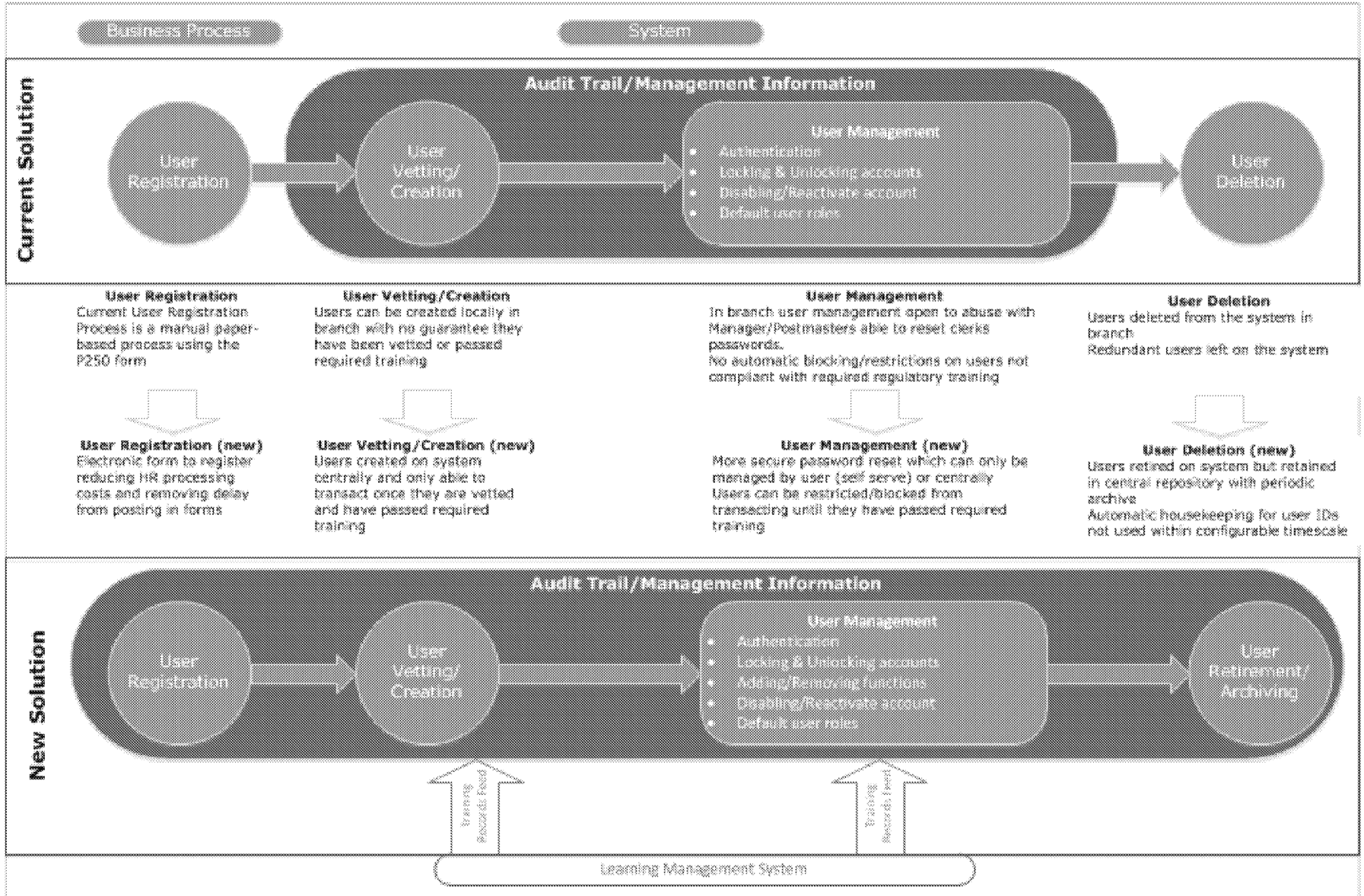
- No control of who is in our branches
- No record of who in the branch has been trained to the required standards
- Branch Managers can currently control users and change their passwords
- No single, centralised User Directory
- Not all employees in Branch are being correctly vetted
- The process for vetting employees is paper based and slow
- There is no audit trail of activities performed against a user ID in branch

POL00038770

The 'AS IS' issues and recommended 'To Be' state to address those issues is illustrated in the diagram below.

POL00038770

BUSINESS SOLUTION DESIGN DOCUMENT – ENHANCED USER MANAGEMENT V3.0



POL00038770

1.3.1.1.1. Recommendations

The solution must provide:

All users of the Horizon system with a single, unique user ID.

A central repository to house all user credentials for the Horizon system throughout their lifecycle

Confidence at a business level that we know who is working in our branches; that they have all been vetted; had right to work in UK checks; and have all completed the required induction and ongoing regulatory & compliance training.

The ability for POL to isolate user access to Horizon should they fail to pass or complete the necessary training as specified by POL e.g. if a user does not successfully complete AML training/test then access to products such as foreign currency would be switched off centrally within POL

Links to the Learning Management system (Success Factors) to ensure that only staff who have passed the relevant training are enabled to serve customers.

POL00038770

1.3.2. Impact on Core Operating Processes & Management & Support Services

High Level Benefit Assessment

	Enhanced User Management
Direct Cost Savings	+ Estimated £50k p.a. saving if the P250 registration form could be automated **only when/if** link with LMS/compliance training is delivered + Further estimated cost savings Estimated at £70k (figure requires further analysis/validation) saved by Branch Standards Team _ HR have raised a risk based on the requirements that they would need to put in additional resource to manage creation and administration – to be validated
Avoided Costs	+ Further potential benefit achieved through the consolidation of password management. + Branch staff only allowed to transact if they have completed mandatory, regulatory training therefore removing risk of financial penalties. • Example: Data protection Act 1998, Principle 7 indicates organisations must provide adequate training and education to staff. Failure to demonstrate this could result in regulatory penalties of £500k rising to 5% of turnover in the revised DPA expected to go-live in the summer. Furthermore in the event of an ICO enquiry, failure to provide adequate evidence may result in an audit programme of our branches being forced upon us.
Non Financial Benefits	+ Clearly understanding who has completed a transaction should enable successful prosecution, reduce legal consultancy and reduce the number of mitigation cases. + Linking user management to LMS will give POL an individual training record for each user + Enforcement of necessary vetting and training before allowing users to transact + Mitigation against regulatory and reputational risk against a backdrop of increased scrutiny from some regulators. + Improved controls – end to end recruitment, vetting and access processes

~~**Direct cost savings**~~ ~~• **Resource**~~	~~120.0~~
~~**Avoided costs**~~ ~~• **Financial penalties**~~	~~500.0~~
~~**Non financial**~~	~~• Improved controls – end to end recruitment, vetting and access processes~~ ~~• Assurance provided to 3rd parties – CAA, POCA contract, Royal Mail~~

POL00038770

POL00038770

1.4. Next Steps

The Solutions Design Document has been produced and is being reviewed. A summary has been presented to the SUF and the Sponsor w/c 1 August.

1.5. Owner

This document is owned by Angela Van Den Bogerd who is responsible for approval of this document and all related feedback should be directed to them.

2. Business Context

In accordance with Post Office Information Security Policy and adverse risk appetite, Post Office's key controls are designed to ensure regulatory compliance and to make sure we appropriately manage who has access to data. Policy requirements include:

- Post Office Acceptable Use Policy V1.0 (Section 5 access management refers)
- Post office Business Information systems Policy V1.0
- Post Office Cyber Information security Policy (section 5.6 human resources security section refers) V1.0
- Post Office Information Assurance Policy V1.0
- Post Office Data Protection Policy V3.0

2.1. Background

We have an opportunity to decrease risk and improve controls of User Access and subsequent User Management of the Horizon system. In preparation for tender for the Front Office Tower an improvement opportunities log was compiled and table 1 of section 2.2.1 below is an extract of the improvement that were identified which relate to user management.

In addition, Project Sparrow produced a number of improvement opportunities which relate to User Management which are detailed section 2.2.2 below.

2.2. Business Problem

The present user management solution does not provide the necessary controls over who can access and transact on the Horizon system, thereby exposing the business to regulatory, financial and reputational damage.

Sections 2.2.1 and 2.2.2 highlight the improvement opportunities that the business has identified through the Front Office Tower procurement exercise and also from Project Sparrow.

2.2.1. Problem Statement

There are two main classifications of the business problem with User Management in the Horizon system today:

POL00038770

1. Lack of control
2. Inadequate risk management.

The current system does not allow the business to control who has access to the Horizon system and what they can do once able to log onto the system. It does not enforce any pre conditions on Users so, for example, Users should have undergone a basic disclosure process via Disclosure Scotland but Users can access the system without this check being conducted and the User being declared clear to use the system.

We cannot stop Users from accessing the system even though they may have convictions for theft or other serious crimes nor can we prevent access where Users have failed to complete a compliance test or have failed that test.

All of the above means that there is considerable risk to the business:

- Risk to Post Office funds from theft, fraud etc.
- Risk to customers' funds due to theft, fraud etc.
- Risk to customers' personal information
- Risk of prosecution for non-compliance
- Risk to Post Office's reputation
- Commercial risk – many client contracts stipulate that branch staff must have completed the disclosure process to transact their products.
- Commercial risk – it is a legal/ regulatory requirement and a client requirement that all colleagues serving customers must have had training and completed certain compliance tests successfully.

Further business problems today include:

- Financial Losses (written-off) as we are unable to fundamentally prove User management was a problem
- We cannot prove that people have been trained (Compliance to provide figures on training)
- We do not have a complete record of all Assistants employed within the Agency Network. (This issue refers to agency branches only.)
- Due to how User Management exists today we can be liable for PCI compliance fines
- We are at risk of reputational damage, as there are risks like staff not being trained sufficiently which can lead to products being mis-sold and compensation payment being made to customers and financial penalties being incurred by regulatory agencies.
- Branch Managers have too much control today in terms of their ability to create new Users and amend existing User details.
- Today's process is very manual and results in a lot of paper having to be manually complete to create a new User (when done in the correct manner)
- Lack of automation – user management will be an enabler for Success Factors to fully automate the Vetting process.
- Colleague offers cannot be monitored via the system today.

POL00038770

2.2.2. Current Mode of Operation Issues

Front Office procurement – extract from improvement opportunities log.

Reference	Description	Process Step Reference
IO_331	Improvements to system wide handling of Users. The requirement of annual reporting and holding of printed compliance test on a branch by branch basis is archaic. Details and records of tests should be held centrally. This can easily be achieved by adding a hidden branch code prefix to User names to compensate for any duplication. This would also allow easier handling of relief PMR.	Create New User
IO_656	The Front Office Application should be accessible to branch staff solely via the use of a unique User_id so that there is a reliable methodology for auditing sessions or transactions with regard to activity on a per-user basis. User_ids should be unique across the entire network. User_ids should be able to be configured by the branch Users to enable ease of use, but should be looked up against a reference table of existing User_ids to suggest an alternative in the case of duplication. Link to Pay Number? Where applicable. Should be able to be linked to HR system.	Create New User
IO_659	The Front Office Application should be able to restrict Users' rights to complete certain transactions defined as being more complex or higher risk so that the exposure to risk associated with these transactions is minimised.	Create New User / User Roles
IO_661	Non-transactional system events such as log-on and log-off should be recorded in a format and platform which can be queried or used to enrich existing reporting so that activity can be reviewed on a branch User basis.	Logging On / Logging Off

2.2.3.

The following recommendations have been made in relation to User Management from **Project Sparrow.**

Area	Issue identified	Rationale for change	Consideration for Front Office
Migration 1.1	Postmaster & Colleagues claim not to be competent with new system prior to "go live".	Postmasters claiming that they were not competent on the system when it went live & training was not sufficient. POL needs to be able to demonstrate that users being trained are the correct users & that they are fully competent and ready for "go live" to mitigate later challenges. Training logs need to be fully maintained to provide accurate records to mitigate possible later challenges.	• Training to be monitored to make sure that where there are competency issues, they are addressed. • Full training records to be maintained with sufficient notes where applicable. • If any additional and/or intervention is required, it must be fully documented. • A check of all Colleagues to be trained must be carried out with HR. • System driven if not registered unable to access system.

POL00038770

1.4	Users in branch set up with the incorrect access levels.	Risk of fraudulent activity in branch. Provides better controls in branch.	• Communication sent to network in readiness for "go live" including guidelines to access levels. • POL person to make sure that branch staff is set up with the correct access levels and user ID.
1.5	Branches not set up with the correct number/appropriate type of stock unit.	Risk of fraudulent activity. Provides better controls in branch, allowing more accountability.	• Communication sent to network in readiness for "go live" including guidelines re: best ways to set up your branch. • POL person to encourage user stock units where practical & appropriate.
3.2	Where existing branch staff is being retained, a formal assessment of knowledge/skills is not completed prior to incoming Postmaster taking over.	Branch staff may not be skilled in full range of branch transactions and procedures; this potentially could lead to branch discrepancies during new Postmaster's learning curve.	• Training records of existing staff to be retained in order that incoming Postmaster is aware they are fully competent on FO.
3.4	No robust training records retained for all training interventions including sign off from "trainee".	POL need to be able to monitor competency across the network. POL need to be able to demonstrate training carried out across the network and maintain documentation. POL need to maintain records for all training/intervention to hi-light issues re: non-conformance and avoid duplication. Demonstrate a business that is willing to invest in all colleagues.	• Complete all training electronically with confirmation of being stored within FO system at branch & back end level. • The availability for branches to access this information readily in branch.
3.7	Users have a higher access level to the system than required.	To prevent fraudulent activity across the network. To enable Postmasters to have better controls in branch.	• System/business rules need to ensure User access is controlled in branch by Postmaster or person with delegated authority of Postmaster. POL needs central view of this.
5.4	Claims that the Postmaster was not aware of the issues in branch.	Principally, Postmasters are responsible for the operation of the branch and wholly responsible for the restitution of losses. Some Postmasters have little involvement or choose to be 'absentee Postmasters'. In such cases, POL needs to ensure that issues are communicated to the Postmaster.	• Greater identification of the user end User. • Contact with NBSC to be recorded as a User ID personal to caller - link with HR and in branch operations. • Recommend that one unique User ID for each employee/Colleague. • Communicate issues to Postmaster via letter/email to personal addresses, if absent from branch. • Greater reliance on Postmaster to communicate changes in branch /staff – this to be linked with frequent/infrequent access to system in branch so

POL00038770

			POL can monitor.

2.2.4.

A series of workshops have taken place to further identify business requirements to address the acknowledged issues and improvement opportunities around User Management. The following stakeholders attended and contributed to the definition of the current process and identification of business requirements which now form the Business Requirements Catalogue. The AS IS process maps that were produced are shown at Appendix D.

Attendee/Reviewer	Area	Role	Attendance Requirement	Workshop 1 - CMS Leadenhall - 09/02	Workshop 2 - Finsbury Dials - 16/02	Workshop 3 - Finsbury Dials - 23/02
Shaun Turner	Programme	Business Readiness Lead	Required	Attended	Attended	Attended
Hayden Gilmore	Programme	Business Analyst	Required	Attended	Attended	Attended
Phil Norton	Programme	Requirements Manager	Optional	Attended	Attended	Did Not Attend
Andy Thornton	Programme	Project Manager	Optional	Attended	Partial Attendance	Did Not Attend
Sally Rush	Programme	Technical Advisor	Required	Deputy Attended	Did Not Attend	Attended
Hector Campbell	HR	Product Owner	Required	Did not attend	Deputy Attended	Deputy Attended
Samantha Williams	HR	Product Owner	Required	Not invited	Attended	Attended
Debbie Ann Young	HR	SME	Optional	Did not attend	Did not attend	Did not attend
Paul Garnham	Network	Product Owner	Required	Attended	Attended	Attended
Angela James	Network	Product Owner	Required	Did Not Attend	Attended	Attended
Rodney Lewis	Network	SME	Optional	Attended	Did Not Attend	Did Not Attend
Betty Amin	Network	SME	Optional	Attended	Did Not Attend	Did Not Attend
Beau Burton	Training	SME	Required	Attended	Did Not Attend	Did Not Attend
Natalie Liff	Training	SME	Required	Attended	Attended	Attended
Dave King	Information Security	Product Owner	Required	Attended	Attended	Attended
Aftab Ali	Security	SME	Required	Attended	Attended	Did Not Attend
Shirley Hailstones	Project Sparrow	SME	Required	Attended	Did Not Attend	Attended
Kath Alexander	Project Sparrow	SME	Required	Did Not Attend	Attended	Did Not Attend
Paul Dann	FSC	SME	BSD Review Only	Not required	Not required	Not required
Kevin Seller	Network	Senior Sign Off	Sign Off Only	Not required	Not required	Not required
Julie George	Information Security	Senior Sign Off	Sign Off Only	Not required	Not required	Not required
Joe Connor	HR	Senior Sign Off	Sign Off Only	Not required	Not required	Not required

POL00038770

A second Series of workshops has taken place with internal POL Stakeholders to agree the desired TO BE processes based on the recommended solution and to further define business rules and more defined requirements.

Attendees at these workshops were

Attendee and Outputs reviewer	Area	Workshop 1 28 June	Workshop 2 5 July
Shaun Turner	Programme	Attended	Attended
Angela Saul	Programme	Attended	Attended
Dawn Brooks	Programme	Attended	On leave
Samantha Williams	HR	Attended	Attended
Debbie Ann Young	HR	Attended	Attended
Christina Duckworth	HR	Attended	Did not attend
Angela James	Network	Attended	Did not attend
Betty Amin	Network	Attended	Did not attend
Natalie Liff	Training	Attended	Did not attend
Dave King	Information Security	Attended	Attended

Separate consultations were made with Chris Hardy from Security and Fraud and Sarah Rimmer in HR.

These were internal process focused workshops, which remained design agnostic and the following processes and business rules and principles were agreed.

Workshop one on 28 June to cover POL Employed branch users

Joiners process – New POL Employee

Triggers:

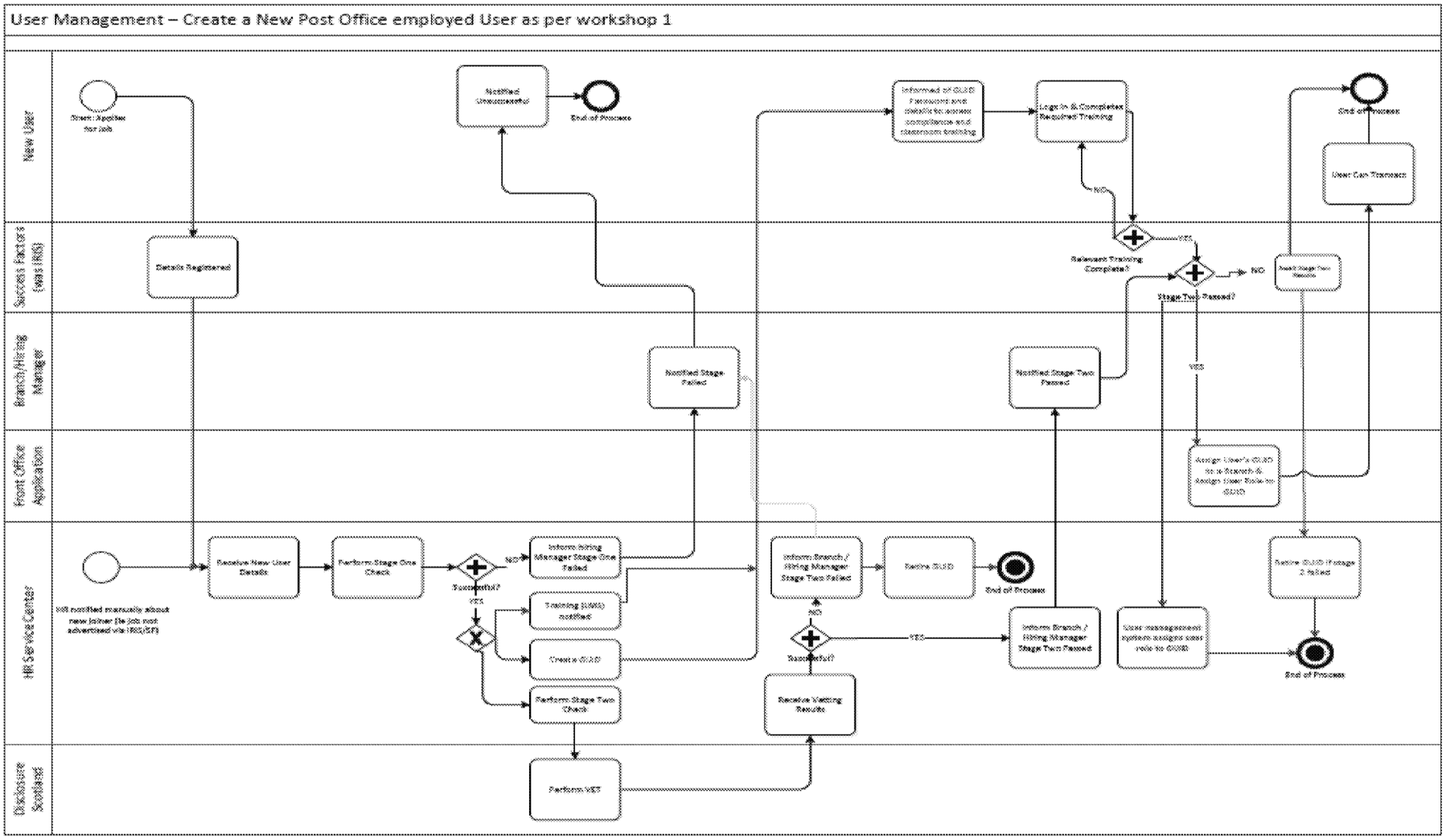
- role advertised on IRIS

High Level Proposed Process Agreed

1. Candidate applies for role via Success Factors.
2. HR gather some initial information from the application, issue invitation for interview
3. Interview takes place and right to work checks and evidence provided during interview
4. Candidate deemed successful and conditional offer made to candidate
5. Candidate confirms acceptance
6. Stage one checks triggered internal - check they've no record in POL bad leaver etc.
7. When stage one passed the **identity is created (GUID)**
8. Candidate can now start using online modules and necessary counter training.
9. Stage two external checks triggered (disclosure Scotland etc.)
10. Stage two passed
11. Counter training passed,
12. User role in user management system updated and pay number created.
13. Begin working in Crown, GUID becomes associated with that Branch.

Note, Full user access to perform tasks in branch will only be granted if BOTH stage two and training is passed.

POL00038770



See separate pdf of process maps embedded at Appendix E for ease of reading –Note: these maps are only concerned with the User Management process steps so do not contain all of the steps undertaken by SF/LMS/HR.

POL00038770

Movers Process – POL Employee

Triggers:

- Staff movement between branches
- HQ staff to work in branch
- Branch staff to work in HQ
- Staff begin working in multiple branches
- Promotion to different role within branch (promotion

The meeting agreed that if we had a single user ID for working in branch then moving between branches would not be an issue ('roaming id'), therefore a process map for Movers has not been deemed necessary. Business Rules to support the requirements have yet to be fully defined or agreed.

Reasons to temporarily disable a GUID:

- Maternity/long term sick leave
- Conduct issue/suspension

(No process map created for movers)

The requirements in the table below emerged during the workshops and form part of the requirements catalogue that is embedded in Section 3. These were shared with both Accenture and Fujitsu and POL prior to the SDD being completed.

POL00038770

Reqt ID	Related High Level Reqt	Version	Functional Area	Functional or Non-functional	Requirement Name	Requirement Description	Reason for Requirement	Acceptance Criteria	Acceptance Method	Priority - MoSCoW	Source
EUM-4.1.2.3.1.1	NEW	3.0	Retention of Data in Audit Log	NFR	Availability of data in Audit Log	Data should be retained for 7 years maximum, It shall be archived after 13 months but access to archive shall be possible at no cost.	Needed to meet Fraud and Investigation team needs in obtaining evidence for court cases.		Statement of Obligation	S - Should Have	Chris Hardy Technical Fraud Analyst
EUM-4.1.2.16.1	NEW	3.0	Create a New User	NFR	Assign a user role - Postmaster / Colleague OR POL/Postmaster	The retention period for previous records of employment with the Post Office/failed applications shall be XXXXXX.	Security	Ability to see all users with a failed CRB application.	Testing	M - Must Have	Workshop 1 on 28 June
EUM-6.0	NEW	3.0	Modify a User	FR	roaming access	The process to attach a user to another branch shall be simple without requiring any unnecessary repetition of data capture	people could be sent to work in another branch for emergencies and don't want to have to go through extensive process of setting that person up almost from scratch in their new branch.	user can be attached to a different branch with minimum amount of data capture. (Depends on the availability of multiple branches on SV&I test rigs).	Testing	should	Workshop 1 on 28 June
EUM-7.0	NEW	3.0	system interface	NFR	system updates	The feed between Success Factors and the User management system shall be as near to real time as possible.	User Management needs to be updated in near real time so that if someone passes their training they are 'unblocked' from performing that task as quickly as possible.	Tests passed in LMS result in updated User Management record within XX minutes. (To be defined).	Testing	Must	Workshop 1 on 28 June
EUM-8.0	NEW	3.0	System Configuration	NFR	System configuration	Attributes in the UM system must be configurable to allow them to be changed according to business wide decisions.	If a new function (such as sell ice cream) or a new attribute is required due to operational changes being implemented then Post Office require this enhancement to be made in XX working days (to be defined but no longer than 5).	A new function or attribute can be added to the system which then allows that function or attribute to be added to all or any user within xx days of creation.	Testing?	Must	Workshop 1 on 28 June
EUM-9.0	NEW	3.0	Modify a User	FR	unattach from closed branch	All staff in a branch where the manager has been suspended and the branch is to remain closed for a period of time must also have their ability to log on at THAT branch suspended.	if there has been fraudulent activity in a branch, simply removing the manager may not be enough. if all staff are re-assigned under the new management any subsequently fraudulent activity can be noted as attributable to the staff member directly and not related to the actions of the	Central admin function (to be agreed where this sits) can de-activate the logon (HUID) of all staff in a particular branch.	Testing	Must	Workshop 1 on 28 June
EUM-10.0	NEW	3.0	Modify a User	FR	unattach from closed branch only	branch staff that have had their logon for a particular branch suspended due to the postmaster being suspended and that branch subsequently remaining closed, must not have their ability to logon in other branches suspended.	Must allow staff who work in multiple branches to be able to work in all other branches they are assigned to except the one that has been closed.	Plural branch users can continue to work in other branches even once their HUID in a closed branch has been centrally disabled.	Testing	Must	Workshop 1 on 28 June

POL00038770

Leavers Process – POL employee

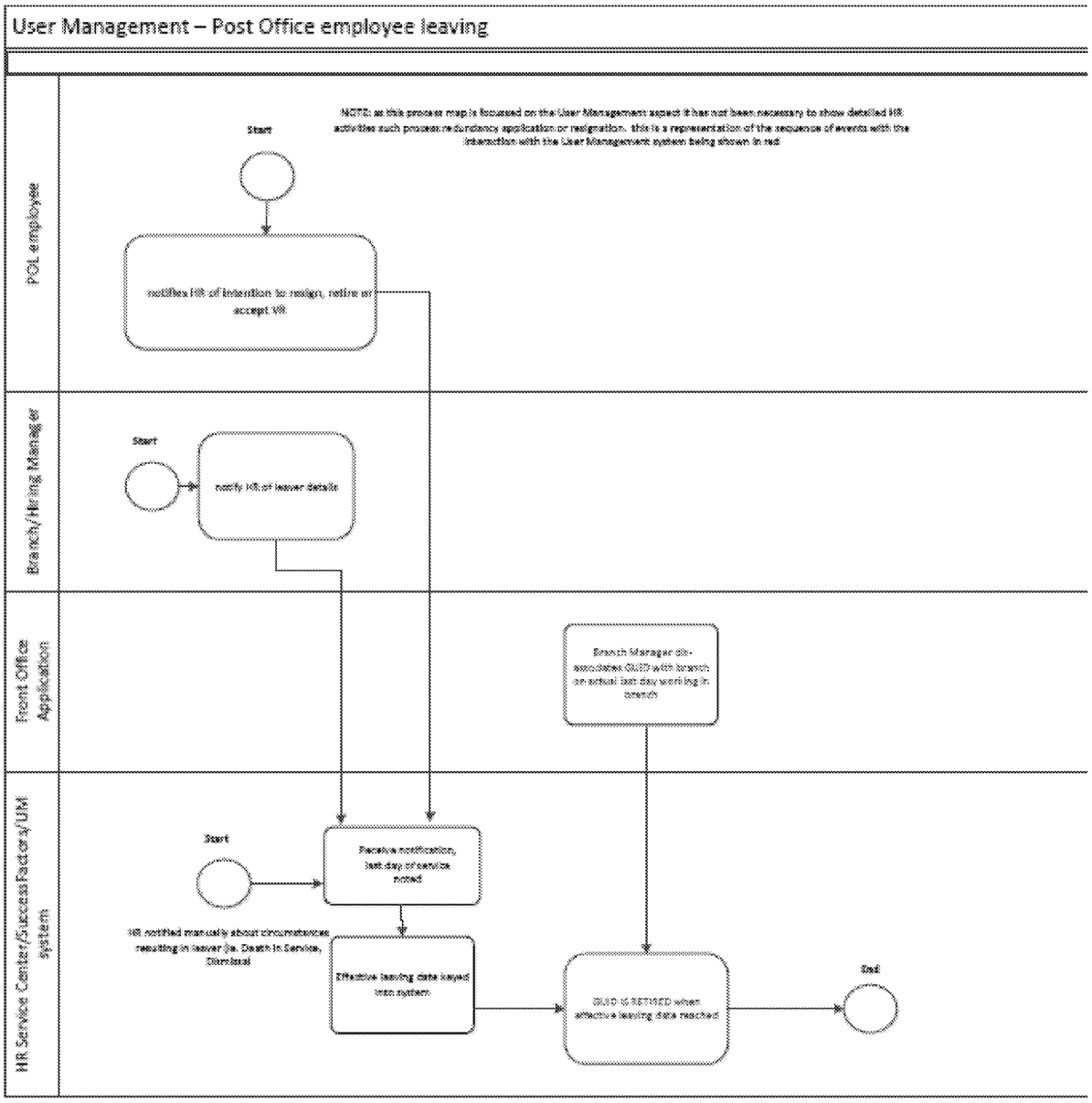
Triggers:

- Death in service
- Suspension
- Redundancy
- Resignation

HR will need to key the effective leaving date into the User Management system. When that date is reached that is when the GUID is retired.
Business Rules to support the requirements have yet to be fully defined or agreed for example, there may be an operational reason why a GUID might not be retired at the leaving date, for example to assist in balancing or accounting processes, however the branch manager should dis-associate user with his branch on their last working day so that for the avoidance of doubt no further transactions can take place under that user Identity.

The central admin function receive a 'hook' out of the SAP system to retire the GUID once all systems have closed the user down.

POL00038770



See separate pdf of process maps embedded at Appendix E for ease of reading –Note: these maps are only concerned with the User Management process steps so do not contain all of the steps undertaken by SF/LMS/HR.

Workshop two on 5 July to cover Postmasters and Postmaster's assistants.

Joiners process – New Postmaster

Triggers: subpostoffice opportunity advertised

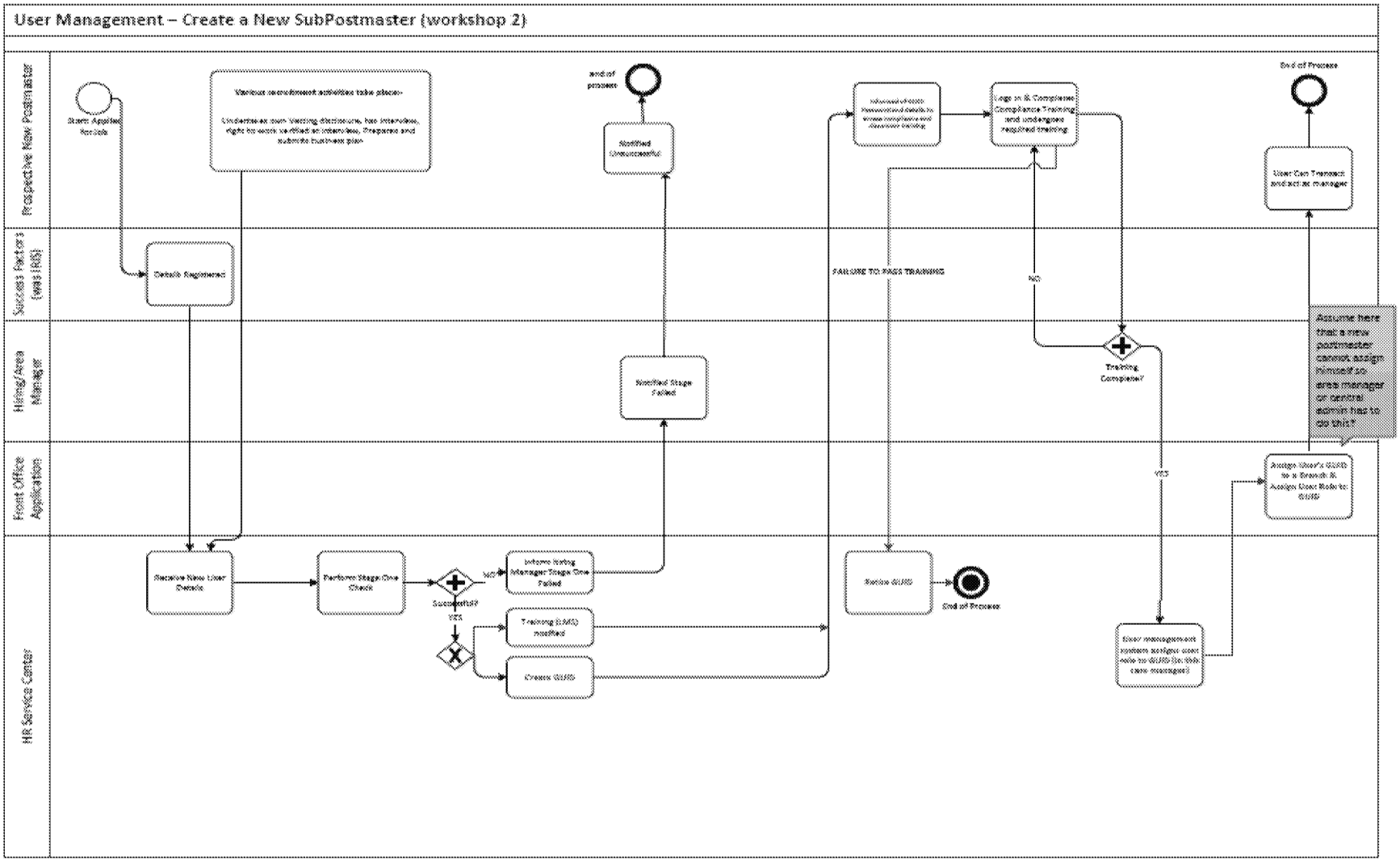
Proposed Process

1. Applies via IRIS or other means depending on commercial opportunities and network.

POL00038770

2. Applicant must have their own stage 2 vetting undertaken as well as Experian checks and submit a business plan to team in Chesterfield. The interview takes place and all of those checks and evidence, including Right to Work are verified.
3. At that point the potential new Postmaster is entered into HR systems and the stage one check is made.
4. Stage one check passed (stage two already carried out at expense of candidate). LMS notified and GUID created to allow candidate to carry out mandatory training activities.
5. Training Passed. User role applied to GUID to allow carrying out suitable transactions for a Postmaster role.
6. First logon in branch is administered by the Auditor/Area Manager present at branch opening.

POL00038770



See separate pdf of process maps embedded at Appendix E for ease of reading –Note: these maps are only concerned with the User Management process steps so do not contain all of the steps undertaken by SF/LMS/HR.

POL00038770

Movers Process –Postmaster

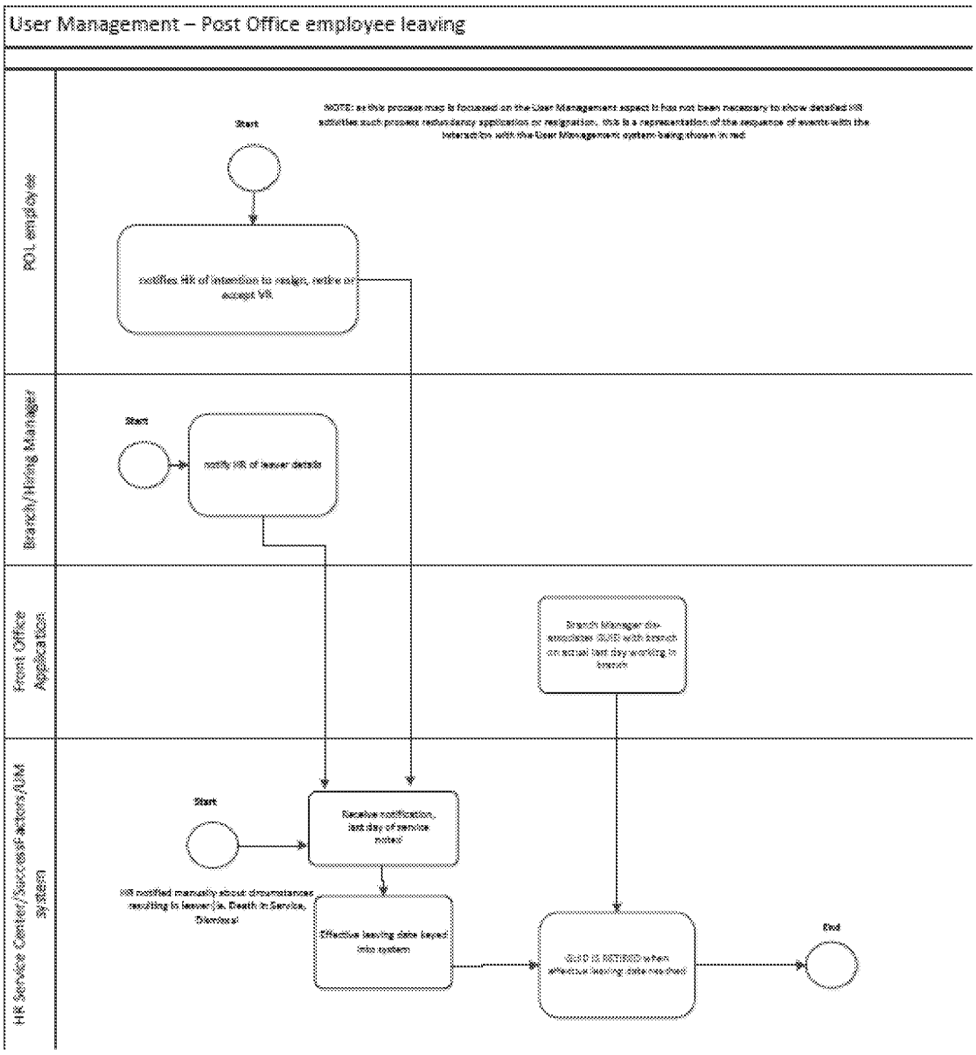
Triggers:
This scenario does not exist. Noted, however, a Postmaster can own more than one sub Post Office and this scenario was not discussed but will be covered further in the Design Phase.

Leavers Process –Postmaster

Triggers:

- Death in service
- Suspension
- Redundancy
- Resignation

The central admin function will receive a 'hook' out of the SAP system to retire the GUID once all systems have closed the user down and any outstanding transaction corrections or debts have been settled.



See separate pdf of process maps embedded at Appendix E for ease of reading –Note: these maps are only concerned with the User Management process steps so do not contain all of the steps undertaken by SF/LMS/HR.

POL00038770

Joiners process – New Postmaster's Assistant

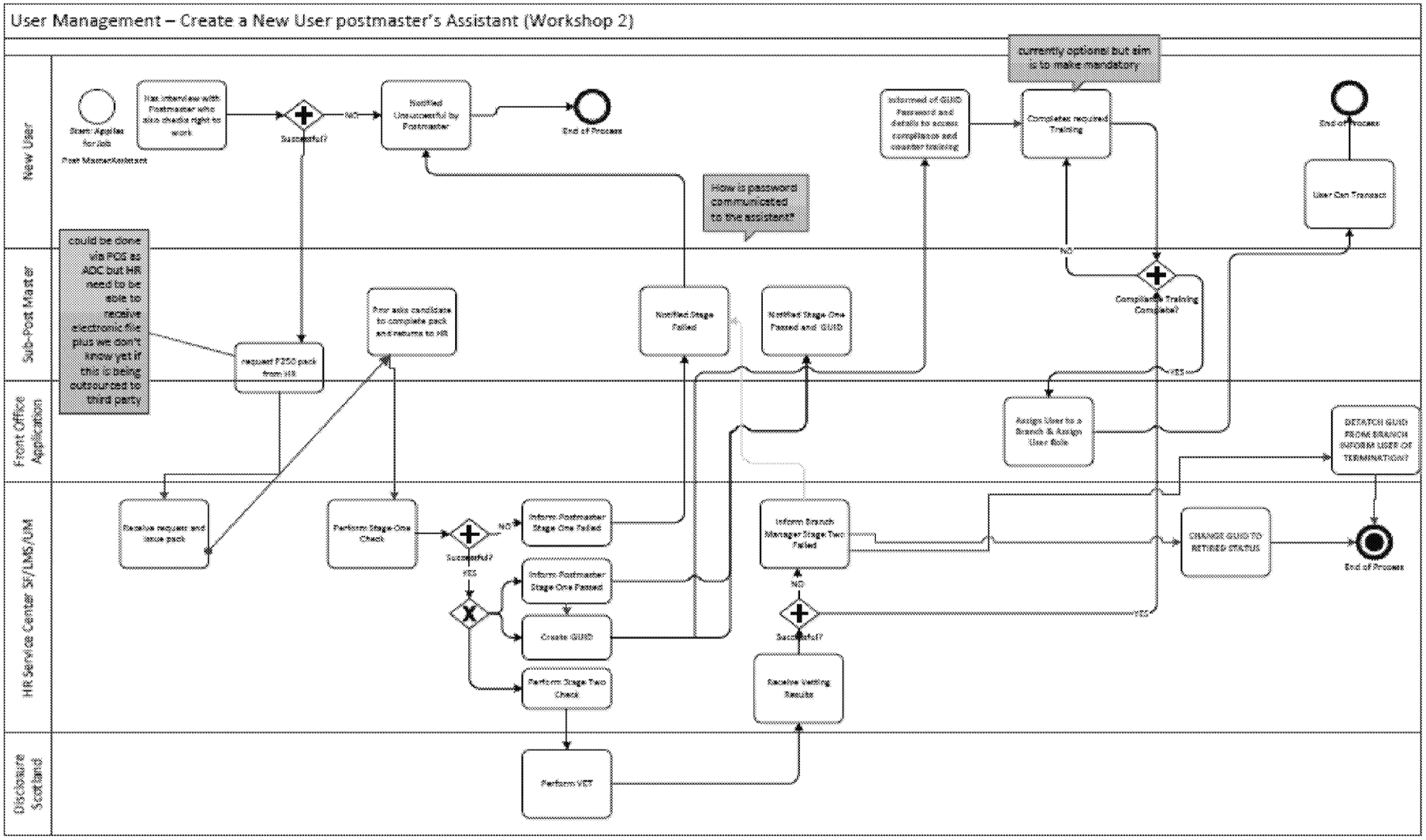
Triggers: needs of Subpostmaster for staffing. Note: advertisement and recruitment is done undertaken through any POL systems and is the sole responsibility of the Subpostmaster.

Proposed Process:

1. Postmaster undertakes interview and right to work checks.
2. Postmaster then contacts HR and requests P250 pack for prospective new assistant.
3. Complete pack returned for Stage One check. User can be allocated GUID and begin training only, no counter transactions.
4. HR conducts Stage 2 checks.
5. As with POL employee only when both successful stage two training and stage two is passed can the GUID be assigned a functioning user role in branch.

NOTE: Currently there is nothing stopping an assistant being given access to serve customers via Horizon before they have stage 2 and any training. In keeping with the aims of the User Management initiative it is proposed that all future processes should always ensure that both training and stage 2 are complete BEFORE an assistant can transact.

POL00038770



See separate pdf of process maps embedded at Appendix E for ease of reading –Note: these maps are only concerned with the User Management process steps so do not contain all of the steps undertaken by SF/LMS/HR.

POL00038770

Movers Process –Postmaster's Assistant

Triggers:

- Staff movement between branches (postmaster may own more than one branch and the Assistant can work in any of them)

Single user ID enables this without any further process needed.

Leavers Process – New Postmaster's Assistant

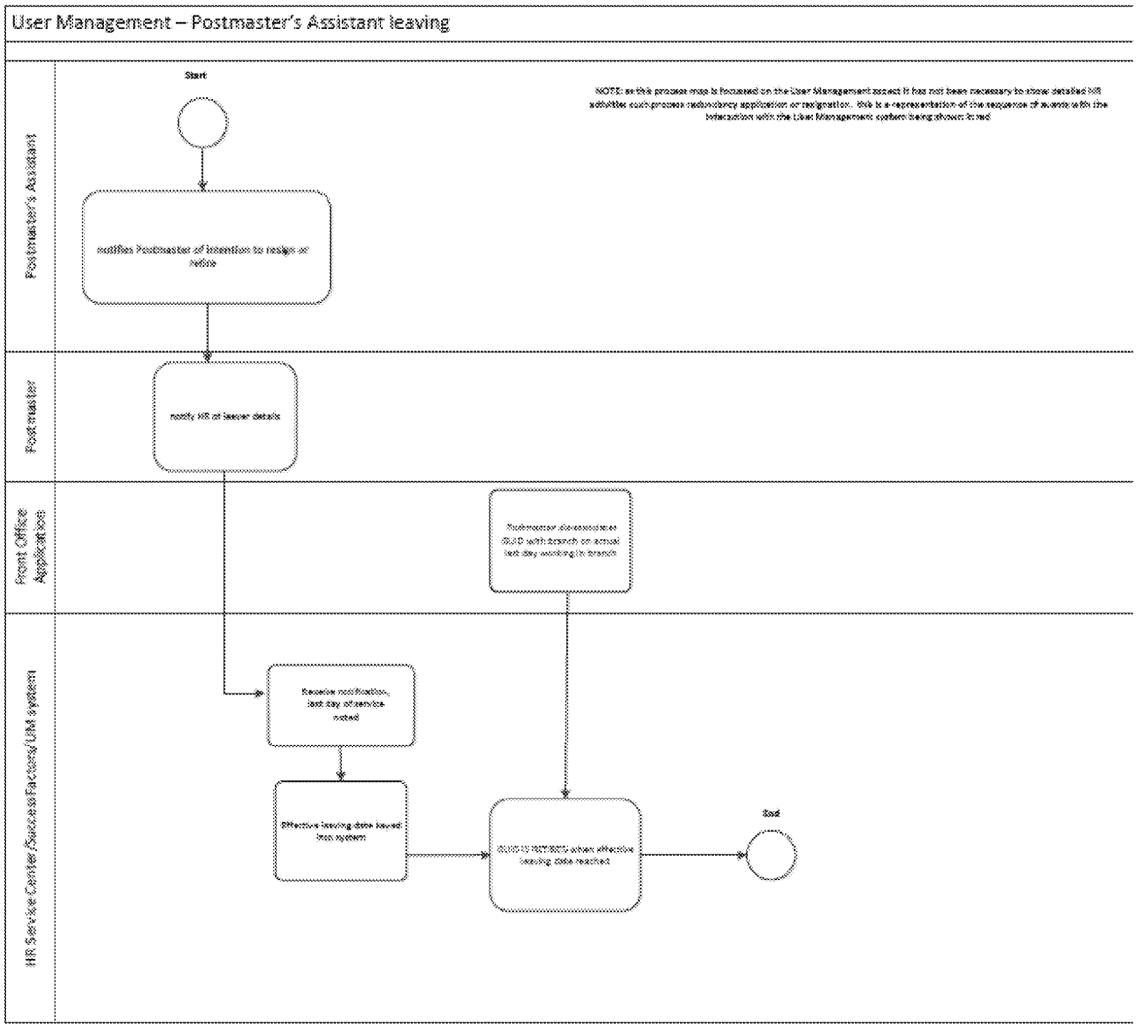
Triggers:

- Death in service
- Suspension
- Redundancy
- Resignation

Note: In ensuring that a Postmaster's Assistant must have stage one and two checks and training confirmed prior to transacting this will ensure they are registered but it can still be the case that a Subpostmaster doesn't inform POL that an assistant has been dismissed/retired etc.

The proposed new process is that a Subpostmaster should inform HR in order that the GUID can be retired. This does introduce a new responsibility for the Postmaster and any process changes or contractual implications have not yet been discussed or agreed concerning this.

POL00038770



See separate pdf of process maps embedded at Appendix E for ease of reading –Note: these maps are only concerned with the User Management process steps so do not contain all of the steps undertaken by SF/LMS/HR.

There are a Set of default **user roles** shown in the table below which have a hierarchical order i.e. branch user reports to branch supervisor who reports to branch manager.

There is also a set of **functions** (also shown in table below) which can be applied to any of the default user roles (includes what product sets they can transact, which stock units the user can attach to etc.)

Within branch a 'branch manager' role can restrict or increase the functions applied to each of his users.

The creation of a new **function** to apply to a **user role** such as selling ice cream would be under taken centrally with the user role being created in the user management system).

POL00038770

Proposed DRAFT User Roles v Functions Matrix (not yet confirmed/agreed)

	LOCAL USER			Support Function *				HR CENTRAL
Function	**Branch User**	**Branch Supervisor**	**Branch Manager**	**Auditor**	**Trainer**	**Support User**	**Engineer**	**Admin Role**
Mails	X	X	X	X	X	X		
Banking	X	X	X	X	X	X		
FSC	X	X	X	X	X	X		
Bill Pay	X	X	X	X	X	X		
Retail	X	X	X	X	X	X		
REM In	X	X	X	X		X		
Rem Out	X	X	X	X		X		
Stock Unit Balance	X	X	X	X		X		
Office Balance		X	X	X		X		
Cash Declaration	X	X	X	X		X		
Stock Declaration	X	X	X	X		X		
Branch Level Stock			X	X		X		
Assign Role			X	X		X		
Add Function			X	X		X		
Remove Function			X	X		X		
Create User			X	X		X		
Archive User			X	X		X		
Disable User			X	X		X		
Enable User			X	X		X		
Reset Password	X			X		X		
View Branch Users		X	X	X		X		
View User		X	X	X		X		
View Sales		X	X	X		X		
Read Only							X	
Create User ID GUID								X
Disable GUID								X
Retire GUID								X

*** is currently named Global User –**The purpose of the Global role type is to give a nominated individual a permanent, personalised Global User account to access any branch on the Post Office estate. A Global user account can be used in any Post Office Branch. The only exception is a Global User ID with the 'Trainer' user group, which can only be used in a Counter Training Office.

There are several types of Global User accounts:-

Auditor E (Emergency Manager)	Gives access to all functions of a Branch Manager and some additional privileges
Migrate Manager	Specialised role for adding new Branches to the Network

POL00038770

	and creating the Local Users for the new branch
Setup	Equivalent to a Branch Manager
Support	Provides limited back office functions
Engineer	Allows access to system diagnostic functions
Trainer	For use on the Counter Training Office (CTO) estate only. The account allows the user to reset the CTO training data.

NOTE *It is proposed that the term Global User shall be discontinued as the solution described later in this document is based on the use of a GUID or Global User ID and confusion could arise. Once the project enters the design phase this issue will be addressed and the above table will be discussed and amended as necessary with the relevant business stakeholders.*

2.2.5. Current Operation Description

During the first set of User Management workshops the existing business processes were documented. For some of the processes (which are more complex) a process diagram was produced (see Appendix D), others which are more straightforward are simply listed as the associated requirements in the requirements catalogue.

Note 1: **Northern Ireland Branches: -** The two processes above are based on Disclosure Scotland Checks being performed on the applicants, should an Access NI check need to be performed the process is as follows:

- P250 received in HRSC (this will be replaced by the automated data capture of this data onto a portal and automatically sent to HR)
- Stage 1 pass letter sent to Postmaster – including link and PIN number. (this will become an electronic notification)
- Colleague logs into Access NI system and fills in relevant data
- HRSC approve
- Access NI complete checks and return Certificate to HR

Note 2: **BFPO** – It is acknowledged that BFPO's use their own set of business rules to create new users and the work undertaken to date has not yet covered these activities in sufficient detail. There is a general aim to bring the BFPO processes in line with POL ones but that may not be possible and therefore there may be an additional number of requirements relating to the BFPO as work progresses during August 2016.

POL00038770

2.3. Scope Boundaries

2.3.1. In scope

In broad terms the scope of the work package can be summarised by the following two areas:

- **End-to-end User life cycle management**
- **Access control**
- **User Compliance**

End-to-end User life cycle management- This document includes the processes related to management of a system User, from the initial registration and set up, through any amendments and changes once the User is enlivened and through to the end point for a User when they are archived from the system.

Access control defines the attribute which can be assigned to a User which determines what the system functions a User can access and action. This manifests itself in the defining of User Roles (Section 3), which are essentially default groupings of attributes determining the system functions which are accessible to a User.

User Compliance – The Branch Standards team in Support Services are regularly called on to supply Management Information regarding Branch Users and the products they have sold. For example, A forthcoming Audit by the Civil Aviation Authority means that the Branch Standards Team have to use 20 FTE's for one month to gather and validate data on branch users that have sold mails products to ensure that they have completed the mandatory compliance training. The business has similar responsibilities to demonstrate compliance to Royal Mail, Financial Institutions and other regulatory bodies.

In system terms, the scope of this work package is restricted to Users of the Horizon system. Users are users requiring access to Horizon to serve customers, perform back office functions (e.g. balancing) or system diagnostics. Presently Horizon is access via EPOS terminals in the POL branch network, though if alternative channels for accessing Horizon functionality were to be made available in the future (e.g. via a tablet or laptop), then the same User management processes and principles outlined in this document should apply to those channels.

2.3.2. Out of Scope

The table below outlines the **branch systems** which are explicitly out of scope:

System	Description
AEI	The AEI system within branch requires both separate (enhanced) vetting and User management processes. The existing business processes will continue to be used to provide User credentials for the AEI system.
Pay-Station	User management for the Pay-Station terminals will continue to be managed using current processes.
Self Service Kiosks	The Self Service Kiosks which exist in some branches today do not form part of our scope. The control of who uses these systems (from a branch perspective) will be managed by each user branch as it is today.
POL website *External website accessed by general public*	The Post Office website does not form the scope of the requirements of this document. The system is used by external customers and their Username / password is part of online self-service not User management.

POL00038770

Salesforce *Used by FS/MS to manage appointments*	The Salesforce system is currently utilised in some branches for appointment booking, the Users of this system does not form part of this scope.
Head Office IT systems	Any systems that are used in Head Office.

The table below outlines the **processes** which are explicitly out of scope:

Process	Description
Vetting checks content	This document will refer to the vetting checks conducted both by HR (Stage 1) and external bodies (Stage 2), but will not describe the content of those vetting checks.
Third party vetting checks	Third parties like the Ministry of Defence (for BFPO Users) and Fujitsu perform their own vetting checks, which are outside of POL's responsibility and therefore this document also.
Audit & Legal	Audit and Legal requirements will be part of the Audit and Legal work package as such this document will not contain an exhaustive list of these requirements.
Stock Unit Management	Stock Unit Management (apart from Logging into and off a stock unit) will form part of the scope for Branch Accounting.
CTC	Counter Terrorist Check
SC	Secured Cleared process is not in the scope of User Management.

POL00038770

2.3.3. Requirements out of scope

A number of requirements in the Enhanced User Management Business Requirements Catalogue V3.0 have been identified as being out of the scope of Release 1 and more relevant to the Success Factors project. These are being discussed currently to agree ownership and are coloured Amber in the main requirements catalogue document for easy identification.

Reqt ID	Related High Level Reqt	Version	Functional Area	Functional or Non-functional	Requirement Name	Requirement Description	Reason for Requirement	Acceptance Criteria	Acceptance Method	Priority - MoSCoW	Source	Owner
EUM-4.1.2.6	4.1.2.6	3.0	Create a New User	FR	Assign a user role - Postmaster / Colleague OR POL/Postmaster	HRSC must be notified when a new P250 has been received.	Security **(clarification note** - *awaiting confirmation if this requirement can be passed to the SF/LMS project)*	notification appears on first receipt of P250	Testing			Reviewing with Debbie Ann Young as may be SF requirement
EUM-4.9.2.1	4.9.2.1	3.0	View User Information	FR	View User Information	It shall be possible for a User to view their personal information and generate a request for this to be modified, if necessary.	Security - fraud prevention **(clarification note** - *awaiting confirmation if this requirement can be passed to the SF/LMS project)*	Users are able to see their own personal information and make a request to modify it through an auditable channel	Testing	Should	Stakeholder workshops and BSDD	Reviewing with Debbie Ann Young as may be SF requirement
EUM-4.9.2.3.2	4.9.2.3.2	3.0	View User Information	FR	View User Information	It shall be possible for support functions to have access to the updated training records for each user via the User Management System	Security - Compliance **(clarification note** - *awaiting confirmation if this requirement can be passed to the SF/LMS project)*		Testing	Must	Stakeholder workshops and BSDD	Reviewing with Debbie Ann Young as may be SF requirement
EUM-4.9.2.4	4.9.2.4	3.0	Modify a User	FR	Modify a Users Details	It shall be possible for a User to view their training history through the POS	Security - Compliance **(clarification note** - *awaiting confirmation if this requirement can be passed to the SF/LMS project)*	Users are able to see their own training history via the POS	Testing	Must	Stakeholder workshops and BSDD	Reviewing with Debbie Ann Young as may be SF requirement

POL00038770

2.4. Problem Impact on Business

The problems described within this document manifest themselves as follows

2.4.1. People

Branch Manager/Postmaster – There is no way to see if a user has taken and passed the mandatory training modules, and no certainty as to which user has actually used a specific stock unit as there are no controls around users and stock units attached to.
User – There is a risk of password sharing (which will not be totally eliminated by this solution) which means that Post Office is unable to take action against the correct person.
HR staff – There are lengthy paper based processed to vet potential employees and return findings to Postmasters. The current solution is stand-alone, potentially incomplete and subject to regular verification exercises.

2.4.2. Process

The "As Is" processes are complex to perform and have a lack of control and auditability. The current processes are not enforced for all branch users, for example Postmaster's Assistants can use the system without any training and are only put through the vetting process if the Postmaster initiates it. There is a general lack of end to end process integrity.

2.4.3. Technology

The current solution comprises various disparate elements which are inconsistent and lack integration.

The following table, extracted from the SDD, summarises the gap analysis between the current model of operation and the envisaged future model of operation, and illustrates how some of the current business problems will be addressed.

Category	CMO	FMO
Management of unique identifiers.	The user identity management in the current solution is managed by the Horizon system. The primary issue with the current system is that a single user can have multiple identifiers. The unique identifier in the Horizon system is termed as HUID. The primary reason why users have multiple HUID's is because the HUID is a construct of FAD terminal + log id. There are multiple FAD (HNG) terminals within branches and also users work in multiple branches.	In the future mode of operations the user will have a global unique identifier – GUID maintained and managed by the new enhanced user management system. The GUID will be mapped to the existing multiple HUIDs during the migration process. Also the GUID will be mapped to the SAPID of the user managed within the HR SAP / Success Factors.
Types of user information stored within different systems.	The Horizon system stores the information about the users primarily from the branch perspective. The types of users that are stored within the horizon system are: • Branch Managers • Branch Assistants	In the future mode of operation Horizon system will continue to store information about the types of users that its stores now. The Enhanced User Management System and HR SAP / Success Factors will store the

POL00038770

Category	CMO	FMO
	• Colleagues The HR SAP stores information about the following types of users. • Corporate Users • Branch Managers • Colleagues The HR SAP does not store any information about the branch assistants.	information of all four types of users. • Corporate Users • Branch Managers • Branch Assistants • Colleagues
User credentials	The user credentials (username/password) are stored within the Horizon system in its central database. No user credentials of any kind are stored within the HR SAP system	The Enhanced User Identity and Access Management system will be the primary system that will create and manage the user credentials for all types of users. During the interim phase the users that have not be migrated to the enhanced user management system will continue to use the credentials from the Horizon system. For all new and migrated users the credentials will be maintained centrally within the enhanced user management system. The Horizon system will have the capability to validate the credentials with the central enhanced user management system during user authentication process. HR SAP / Success Factors will not maintain any user credentials.
User Lifecycle management & Role assignments.	In the current system the user life cycle management is done by the branch managers within the Horizon system. A single user may have multiple ids within the same or across multiple branches. This is because the branch managers manage this process within the local branches. All the role assignments is done through the HNG terminals.	The user lifecycle process will be stream lined through HR Success Factors and Enhanced User Management System. In the interim state the enhanced user management system is assumed to be the master of user life cycle management information and will maintain the different states including role assignments. HR Success Factors will eventually become the master of user lifecycle management and will be responsible for providing updates to the Enhanced User Identity & Access Management system. Whenever roles are assigned through HNG terminals the Horizon system will be responsible for sending the updates to enhanced user management system.
Authentication & Authorisation	The authentication and authorization is managed by the Horizon HNG terminals where the credentials are verified against the Horizon central services.	The Horizon system will delegate the authentication services to the central enhanced user identity and access management system where the credentials are stored. The enhanced user management system

POL00038770

Category	CMO	FMO
		will provide the role details and other attributes to the Horizon system to perform access control. If the user has multiple roles across multiple branches he will prompted to select a role and branch from where he would like to perform his operations post authentication process.
Self Service	There are no self-service features in the current mode of operation for users to change his password. User passwords are reset by the branch managers. The risks with the existing system is that branch managers are aware of their assistants' passwords.	The enhanced user identity and access management system will provide the services for users to change the password in scenarios when he is a new joinee and also when he has forgotten his password. The self service capability will also provide the features for user to set and validate the security questions during password resets. In scenarios where user is unable to answer the security questions accurately capabilities will be provided within the enhanced user management system to service the user with password resets through a help desk function.
Password Policy	There is currently no password policy managed within the Horizon system in the current mode of operation.	The enhanced user identity and access management system will enforce a password setting policy within the system for the users. For example. • Minimum of 8 characters. • Should contain alphanumeric and special characters. • Should have at least one character in caps. There will be administrative interface to configure the password policy. The system will also have the capability to configure other rules. Examples of certain rules are listed below. • User will be forced to change his password periodically. • User cannot repeat his password for at least 12 consecutive changes.

2.5. Solution Constraints

In accordance with Post Office Information Security Policy and adverse risk appetite, Post Office's key controls are designed to ensure regulatory compliance and to make sure we appropriately manage who has access to data.

Constraints on the required solution are:

Constraint	Description

POL00038770

Constraint	Description
Timescale	Implementation of a full end to end solution is dependent upon the development of links between the User Management solution and Success Factors The impact of HNGa rollout on implementation has yet to be determined.
Resource availability	Resource requirements are defined in the business case
Budget	Authorisation and budget will be determined by Post Office governance
Legislation or Regulatory needs	There are no legal or regulatory constraints, although there are a number considerations and requirements which need to be met.
Technology framework/strategy	Solution components must provide the capability to operate within the constraints of the domain ownership rules of the Information Model. There are constraints within the Horizon system to provide this functionality hence this capability will be provided through User interface provided by the enhanced user identity and access management system for the POL users.
Company Standards	Post Office Acceptable Use Policy V1.0 (Section 5 access management refers) Post office Business Information systems Policy V1.0 Post Office Cyber Information security Policy (section 5.6 human resources security section refers) V1.0 Post Office Information Assurance Policy V1.0 Post Office Data Protection Policy V3.0
Security	Defined above and to be determined
Safety	No constraints envisaged

2.6. Solution Acceptance Criteria

To be determined in the design phase of the programme.

The following key success factors represent measurable criteria that will be used to evaluate the recommended solutions to determine a solution will be acceptable to the business.

Id	Description	Measured by
SOL-1		

2.7. Key Stakeholder Needs

The key solution needs from the perspective of key Stakeholders are:

Area	Stakeholder Name	Key Needs/Features of solution
People	Angela Van Den Bogerd Joe Connor Gayle Peacock	• *Clear accountability and resource needed to support Branch Messaging and Help & Support* • *Changes to roles in HR, Communication, NBSC and Product Managers to support effective end to end business process to determine suitability to serve customers* • *Users uniquely identifiable* • *Users Training and Compliance can be proven*

POL00038770

Area	Stakeholder Name	Key Needs/Features of solution
Processes	Angela Van Den Bogerd Joe Connor Gayle Peacock	• *Tighter controls around vetting to determine ability to transact only when trained* • *Revised business processes with links maintained between training status and system access*
System	Angela Van Den Bogerd Joe Connor Gayle Peacock	• *Passwords created centrally and not by end users, with password supplied to end user* • *Management of new supplier with new support arrangements, continuity and DR* • *Information is shared in real time*
Policy/ Standards	Dave King Chris Hardy Angela Van Den Bogerd	• *Policies to be clearly defined and communicated – particularly to agents/operators/postmasters* • *Data retained in line with legal and business requirements*

3. High Level Stakeholder & Detailed Requirements

Name	Area	Role	RACI Responsible Accountable Consulted Informed
Hector Campbell	HR	Product Owner	Responsible
Samantha Williams	HR	Product Owner	Responsible
Debbie Ann Young	HR	SME	Consulted
Christina Duckworth	HR	SME	Consulted
Sarah Rimmer	HR	SME	Consulted
Paul Garnham	Network	SME	Consulted
Angela James	Network	SME	Consulted
Beau Burton	Training	SME	Consulted
Natalie Liff	Training	SME	Consulted
Dave King	Information Security	SME	Consulted
Chris Hardy	Security	SME	Consulted
Shirley Hailstones	Project Sparrow	SME	Consulted
Kath Alexander	Project Sparrow	SME	Consulted
Caroline Hilton	Product Manager		Informed
Martin Kearsley	Project Manager		Informed
Alison Jaap	Target Operating Model owner		Informed`
Stephen K Ward	Branch Standards		Informed

The detailed Requirements Catalogue is embedded below.

Enhanced User Management_Busines

4. Functional Use Cases

TBC in Design Phase

This section defines the functional requirements in terms of the system actors and outline use case/functional descriptions.

POL00038770

Use Case
Templatev1.0100915

<Insert completed 'Use Case' document here >

5. Recommended Option

Option 2 – Off the Self (Preferred)

5.1. Summary

Phase 1 - Off the shelf solution – no integration with HR system

- Off the shelf package procured and integrated with Horizon
- Could support single sign on to other systems in POL estate
- Delivers benefits whilst de-risking Success Factors implementation. Can be plugged into Success Factors in phase 2
- Likely automation of P250 process in HR,, current database replaced, but dual running of processes until Success Factors implemented

The Enhanced User Identity and Access Management will integrate with the Horizon System by providing the following capabilities.

Authentication Services: The users of the Horizon System will be authenticated using their credentials (username / password) stored within the Enhanced User Identity and Access Management System.

Access Control Services : The Enhanced User Identity and Access Management system will provide information about the authenticated user to the Horizon system in the form of web service call about which branches does he belong to and what are the active roles within those branches. The Enhanced User Identity and Access Management system will also provide the status of the user's training based upon which the Horizon system can perform the necessary authorisation to allow or disallow users to use certain functionality within their systems.

User Lifecycle Management & Role Assignments: The Enhanced User Identity and Access Management System will provide the web service interface to the Horizon system to manage the lifecycle of user in terms of Role Assignments. For example when the Branch Manager changes the role assignment for the user within the Horizon System, the Horizon system will notify the Enhanced User Management System with the updates and the vice versa.

The Enhanced User Identity and Access Management System will integrate with the HR SAP initially and later with Success Factors – Employee Central modules to acquire information about the user's onboarding and background check status.

The HR SAP / Success Factors will notify the enhanced user identity and access management system about the various status of the users (including the joining and leaving status).

POL00038770

The enhanced user identity and access management is responsible for the following functions.

1. **User Registration**: The new user is registered after the Stage 1 checks (Identity & background checks) are completed by HR. The user registration details are either sent from the Success Factors – Employee Central Module or the HR person will register the new user within the Enhanced user identity and access management system using the user interface.
   The user details are also updated after stage 2 checks (CRB, Disclosure Scotland).
2. **GUID Generation:** The Enhanced use identity and access management system will generate a unique Global user identifier for the new user. The username and password will also be generated for the user to help him log into the Learning Management system to complete his mandatory training.
3. **Role Assignments:** The Enhanced User Identity and Access Management System will provide the capability for branch managers to assign roles to the users. Roles can be assigned through Horizon terminals. If the roles are assigned through Horizon Terminals the Horizon system will notify the Enhanced User Identity and Access Management System. Alternately if the role is assigned through the Enhanced User Identity and Access Management System the EU-IA will have to notify the Horizon system about the role assignments.
   The system must not allow any role assignments if the new user has not completed his basic training through the Learning Management System. The Success Factors will provide this information to the Enhanced User Management System about the training status of the user.

Phase 2 - Off the shelf solution – full integration with Success Factors

- linked to employee creation
- Licences required for full Success Factors integration
- Avoids duplication of people data

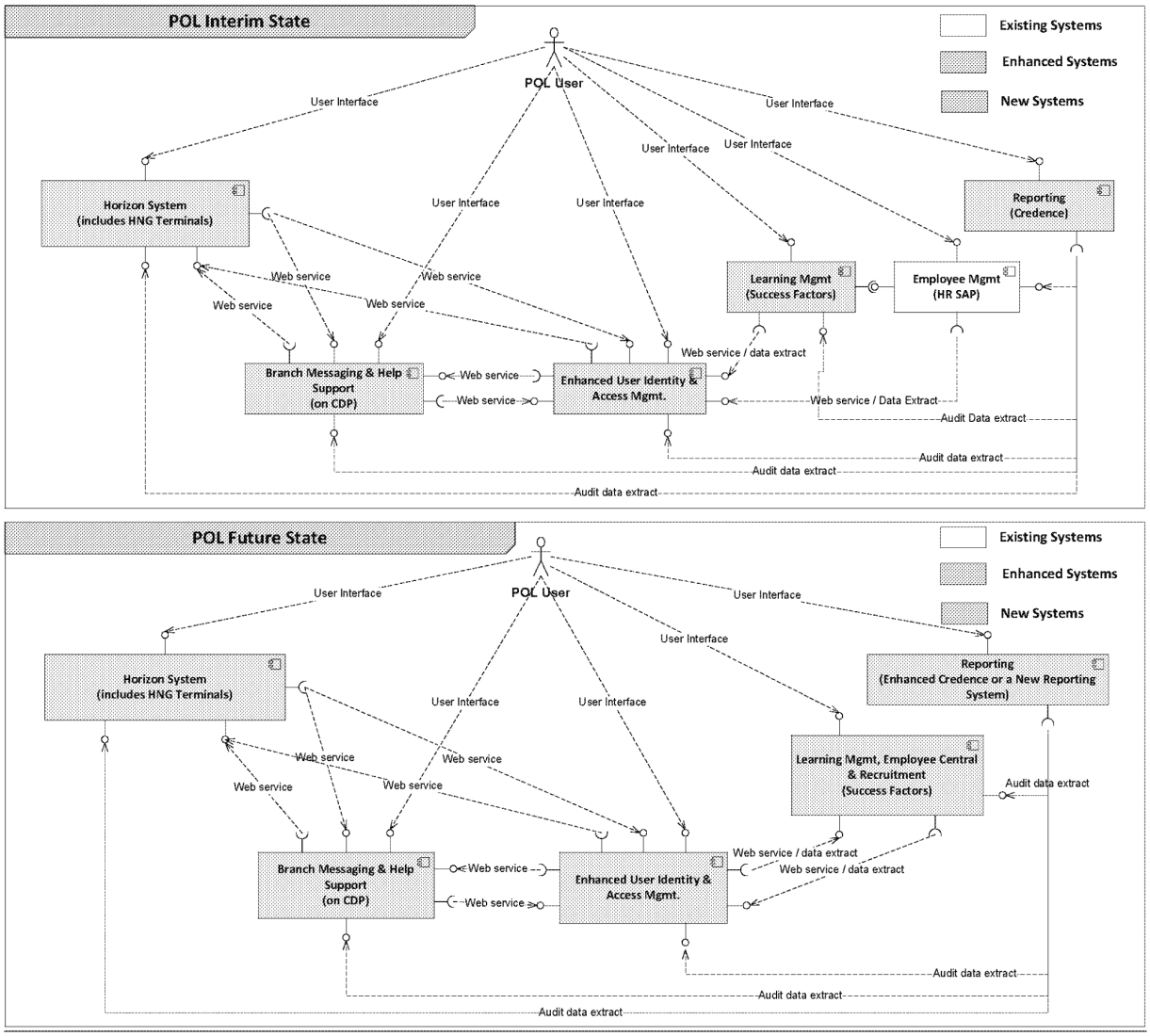
The Success Factors – Learning Management module will integrate with the enhanced user identity and access management system to provide the status of user trainings which will be a key factor in allowing a user to transact on the Front Office Solution.

The key difference between the interim and future state of operation is that the HR SAP ERP system will be decommissioned and will be replaced by the Success Factors which provides the capabilities e.g. Employee Central, Recruitment & Onboarding, Payroll, Performance & Goals and other HR related functions.

In terms of the employee master, during the interim state the Enhanced User Identity & Access Management System will be the employee master and eventually in the future state the Success Factors – Employee Central module will be the master of employee information after HR SAP is decommissioned.

POL00038770

5.2. Solution Outline



The users would be uniquely identified within the EU-IAM - Enhanced User Identity & Access Management system with their GUID – Global unique identifiers. The EU-IAM is the primary generator and owner of this global unique identifier for the users.

The EU-IAM will also be maintaining and managing the linking between the GUID and the SAPID maintained within the HR SAP/ SF Employee Central. The EU-IAM will also be maintaining and managing the linking between the GUID and the Horizon UIDs. SAPID's are generated within the HR SAP/ SF Employee Central system whereas the HUID's are generated and maintained within the Horizon Central BRDB.

The following diagram illustrates the relationship between GUID, SAPID and HUID.

POL00038770

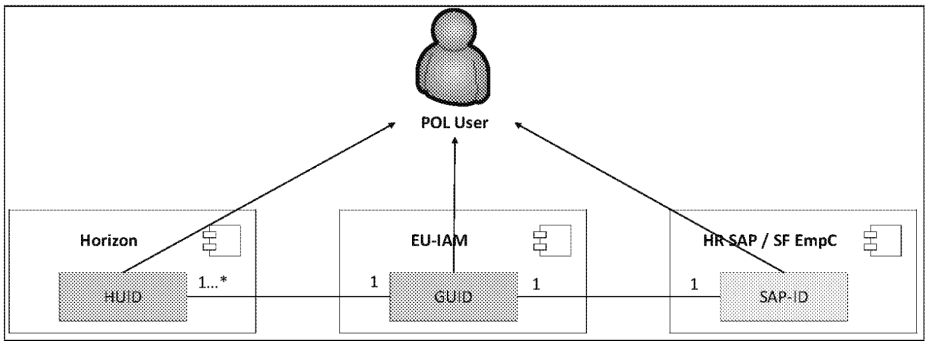


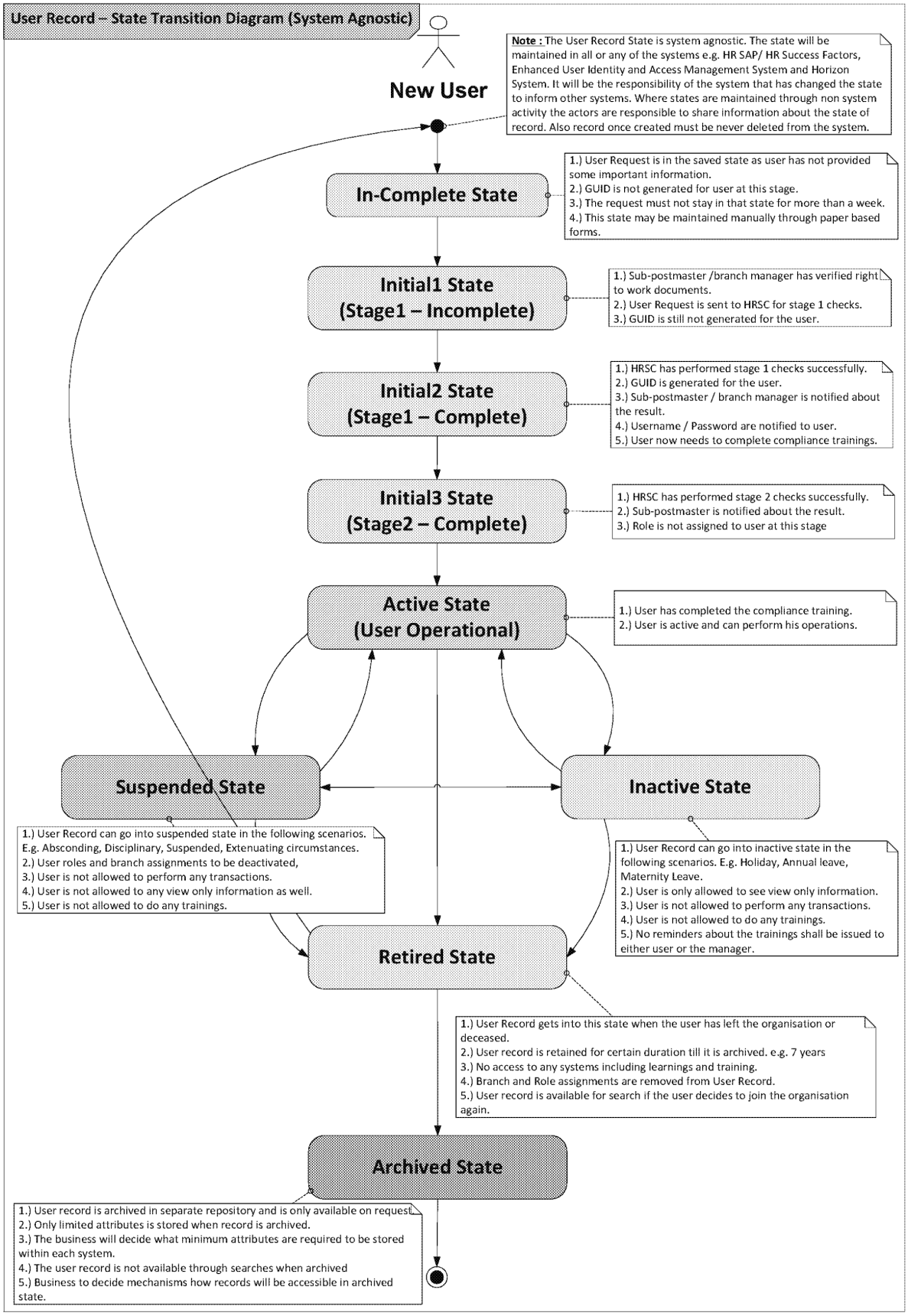
Figure 1: Linking between GUID, SAPID and HUID

As highlighted in the diagram above there will be one to one mapping between GUID and SAPID as both the systems uniquely identify the individual whereas there will be one to many mapping between the GUID and HUID. This is primarily to cover the capability within Horizon legacy system where the single user has multiple HUID's. Although this will not be the scenario when the new users are created when EU-IAM is commissioned. All new users that will be created when EU-IAM is operational will have a one to one mapping between GUID and HUID.

The following diagram describes the different states of the User Record. The user state diagram illustrated below is system agnostic. The user record state will be maintained in either one or many system e.g. Horizon, Enhanced User Identity and Access Management and HR SAP.

It will be the responsibility of the each system to manage the synchronization and reflect the correct status of the user record.

POL00038770



POL00038770

The following table explains the various states of User Record illustrated in the diagram above.

User Record State	Description
In-Complete State	This is the initial state which the user details are captured in the paper based form or the HR system. The new user has provided insufficient details without which the HR cannot perform his basic background checks e.g. identity and right to work checks. Hence the user record will be in an in-complete state. Since no useful details have been provided by the user no GUID will be generated by the Enhanced User Identity and Access Management System at this stage.
Initial1 State	This is the first formal state of user record in which all the relevant user details have been captured by the branch manager and have formally submitted to HR for his Stage 1 – Background checks. The branch manager may have done some initial identity and right to work checks by not necessarily his background checks. Hence still GUID is not generated for the user in the enhanced user identity and access management system.
Initial2 State	At this state the HR has completed the stage 1 background checks. The user record is created with in the enhanced user identity and access management system with a GUID. Also the username and initial password is generated for the user for user to log into the Learning Management System to complete his basic & mandatory trainings. User is not assigned with any role hence he cannot perform any operations with the system.
Initial3 State	At this state the HR has successfully completed the stage 2 checks i.e. CRB, Disclosure Scotland checks for the user. The user is still not operational as he has yet to complete his formal trainings.
Active State	Finally the user record attains an Active state when the user has successfully completed Initial2 and Initial3 states. The postmaster assigns the role to the user in the Horizon system and the Enhanced User Identity and Access Management system. The user is operational and can perform his tasks by authenticating into the business systems.
InActive State	The user record will go into an "inactive" state when the user is on annual leave or a long holiday. The user is allowed to only view on information after authentication. He is not allowed to perform any operations on business systems e.g. Horizon. The user can get into active state when the user is back from his long holiday. He still have to go through the trainings if the operation demands for.
Suspended State	The user record will go into a "suspended" state in scenarios when the user is absconding or suspended from work due to disciplinary action or extenuating circumstances. All user branch and role assignments will be deactivated from the enhanced user identity and access management system and the user will be disallowed to authenticate into any system i.e. Horizon, Enhanced User Identity and Access Management System, Learning Management System. The user can still get into active state if the suspension is lifted by authorised personal e.g. HR, Branch Manager.

POL00038770

User Record State	Description
Retired State	The user record will be in Retired state if the user has left the organization or is deceased. The user record will be still available I the system for a certain amount of prescribed time e.g. 7 years to adhere to the POL data retention policy. User will not be able to authenticate into any system. All branch and role assignments will be removed for the user. Only minimum and essential information about the user record is retained within the system. The user record is available for search if the user decides to join the organization again.
Archived State	The user record is removed from all systems including enhanced user identity and access management system and archived in a separate repository and is available only on request. Only limited set of attributes are retained when the user record is moved to an archived state.

5.2.1. Pros and Cons

This option has the following advantages and disadvantages in relation to solving the business problem and delivery against the high level business requirements.

5.2.1.1. Solution Pros

This solution has the following advantages:

Phase 1 - Off the shelf solution – no integration with HR system

- Re-usable component
- Meets all requirements
- Enables more sophisticated relationships to be created around user roles
- Migration costs likely to be lower
- Enables a strategic solution
- May benefit from supplier upgrades and roadmap

Phase 2 - Off the shelf solution – full integration with HR system

- As above
- Enables end to end integration
- Enables links to be made when staff are employed starting with the generation of employment references – Success Factors becomes the place where the GUID is mastered
- Full integration of joiners, movers and leavers process
- Migration simplified

5.2.1.2. Solution Cons

Phase 1 - Off the shelf solution – no integration with HR system

- Increased cost for initial development

POL00038770

- GUID mastered on Off the Self solution
- Some manual processes still required around joiners, movers and leavers
- People are held in 2 places, HR and the COTS solution for employees and Agents.

Phase 2 - Off the shelf solution – full integration with HR system

- Some further cost to achieve full integration

5.3. Timescale Outline

Draft Release 1
Design Phase Plan - p

5.4. Budgetary Costs

As outlined in the Business Case

5.4.1. Solution Implementation

Implementation plan not yet available.

5.4.2. Solution On-Going Service Delivery

To be considered as part of the Design Phase

5.5. Key Risks & Issues

The following risks were identified during requirements gathering. These will be consolidated into the existing project risks and issues log which contains a full list of all identified risk and issues which are managed on an ongoing basis.

Id	Description	Impact	Likelihood (H, M, L)	Recommended mitigation
01	**Migration** from the present User Management solution to the new solution will require a mapping of the existing user estate to new user IDs. This may be costly, time consuming and uncover hitherto hidden non-compliance around vetting of assistants	Not yet assessed formally		
02	**Password reset** process in the new solution will require helpdesk agents to validate and reset user passwords (if self-serve fails). Cost and resource implications are not understood at this stage.	Not yet assessed formally		

POL00038770

Id	Description	Impact	Likelihood (H, M, L)	Recommended mitigation
03	The **operational convenience** (albeit non-compliance) of Postmasters/Managers being able to add users to the system without waiting for vetting will be removed. Short-term staffing issues will no longer be able to be resolved in that manner.	Not yet assessed formally		
04	HR are fine to approve the process in principle but would want to have documented that we would not be in a position at this time to outline if there would be a saving as this would depend on the work that would sit in HR i.e. taking the piece on creating the ID for Horizon etc. if we do not move to a fully automated P250 via the system and remain with the 'as is' paper based P250 then we would require funding to complete the larger piece.	Not yet assessed formally		

Additional Risks Identified in the Solution Design Document

No.	Description	Mitigation Action Taken or Potential Impact
Enhanced User Identity & Access Management System		
1.	There is risk that the chosen COTs product for the Enhanced User Identity & Access Management system will not provide or support for certain POL requirements.	Identify the GAPs that will not be supported by the COTS product. Assess the priority of the requirement. Assess whether this capability can be provided by custom and alternative configurations/mechanism within the COTS products agreed with the COTS vendor (to support the custom changes). Identify the residual risks. Estimate the additional efforts (if required) of custom mechanisms and agree with POL before implementation.
2.	There is a risk that systems e.g. Horizon, HR SAP, Learning Management may not support the capability to submit real time information about the user lifecycle and attributes changes to the Enhanced User Identity and Access Management system through web service interface.	Alternative mechanisms to be identified and will be provided within the enhanced user identity and access management solution to extract the information if the COTS product support. There will be a residual risk that the information within the systems will not be consistent and in synch. Estimate the additional efforts (if required) of custom mechanisms and agree with POL before implementation.
3.	The Enhanced User Identity and Access Management System will provide centralised authentication service to business systems e.g. Horizon through web service functionality. During operations there is a risk that connectivity may down between the two systems i.e. Horizon & EU-IAM and branch users may not be able to authenticate.	Alternative authentication mechanisms/capabilities to be implemented within the business systems e.g. Horizon to provide offline authentication mechanisms.

POL00038770

5.6. Next Steps

Step	Date
Solution design published	29 July
Solution reviewed by SUF	4 August
Face to face business readiness assessments completed	1 – 8 August
Consolidated Business readiness assessment reviewed – all queries resolved	12 August
Business case review	18 – 22 August
Business case finalised and papers submitted to TDG	25 August

6. Considered Options

This section provides a summary of other potential options that were considered considered.

6.1. Overview

The study considered the following options and their relative pros and cons:

Name	Description	Pros	Cons
Option 1a	Horizon enhancement – without GUID password protection • Horizon processes largely unchanged, with HUID linked to GUID • No GUID password security • Branch manager requests GUID, manually created by HR • Linkages between HUID and GUID held in Credence • GUID requested at log on • APADC used to capture P250 details, transmitted to HR for likely manual processing • Locked into current supplier	• User has a single identity in new systems (such as LMS) • Possible to report on activity across the estate for a user. • HR validation of GUID creation and who is using Horizon (see Cons) • Integration with HR Leavers and Joiners process (subject to interface between the systems being defined and costed) • Would support integration with LMS • Minimal impact on branch process • BFPO's unaffected • Lowest cost if some requirements are relaxed	• GUID could be used erroneously. • Solution is Horizon centric and difficult to separate • Branch Manager could still misuse a Users HUID by resetting the password in his branch. This would be mitigated by alerts detailed on previous slide. • Migration costs likely to be higher • Around 30 requirements partially met
Option 1b	Horizon enhancement – with GUID password protection • Off the shelf package procured and integrated with Horizon • Could support single sign on to other systems in POL estate • Delivers benefits whilst de-risking	• As above • Protects the use of a GUID by password (still no guarantee that it is the real user using it) • HUID Password changes could be further protected	• As above • Costs more • More requirements met but only another 8

POL00038770

Name	Description	Pros	Cons
	Success Factors implementation. Can be plugged into Success Factors in phase 2 • Likely automation of P250 process in HR likely, current database replaced, but dual running of processes until Success Factors implemented	by requiring the GUID password to be entered.	

7. Appendix A – Glossary

This section lists all terms used in this document.

Term	Meaning
AML	Anti-Money Laundering
AP	Automated Payment
AP-ADC	Automated Payment Advanced Data Capture
BRL	Business Readiness Lead
BTTP	Branch Technology Transformation Programme – the programme for the delivery of the Front Office Application
Clerk	The merchant of the product or service at the Post Office counter
CRB	Criminal Records Bureau
Consumer	The User of the product or service acquired by the Customer
Counter	Post Office Counter where a product or service is acquired by a customer from a Clerk
Customer	The acquirer of the product or service
DVLA	Driver and Vehicle Licencing Authority
EPOS	Electronic Point of Sale – the Front Office Application at a Post Office counter, or Electronic Point of Sale – item
FOA	Front Office Application
FSC	Financial Service Centre – Branch Accounting and Client Enquiries
Item	The product or Service being acquired by the customer or used by the consumer
MagCard	Magnetic Swipe Card
Locked Account	An account which is temporarily unavailable due to user forgetting password)
Disabled Account	An account which is out of use long term such as during a users' maternity leave or long term sick leave but should be reinstated at some future point.
Retired Account	An account that has been withdrawn from active life but must not be deleted for audit purposes and shall never be reinstated for

POL00038770

Term	Meaning
	use.
Function	An activity in branch that a user can be granted or denied access to (for example Mails processing or stock unit balancing).
Locked Account	An account which is temporarily unavailable due to user forgetting password)

8. Appendix B – Document History

This section records the version history of this document.

8.1. Version History

Version	Date	Change Details	Author
0.1	05.04.2016	Outline draft produced	Angela Saul
0.2	10.06.2016	More solution Details included following initial SDO	Angela Saul
2.0	20.06.2016	Simply changed name to V2.0 at request of BTTP for consistency	Angela Saul
3.0	05.08.2016	Further details added to Section 5 following release of SDD and stakeholder workshops	Angela Saul
3.1	11.08.2016	More detail added after consultation with Business Readiness	Angela Saul

9. Appendix C – Post Office Process Classification Framework

<To be advised>

10. Document Control

10.1. Purpose

This document presents the findings of the study into User Management.

***Template Guidance. The document reference naming convention should include the initials BSD representing Business Solution Design followed by the Project Reference Number.*

10.2. Reviewers

	Name	Job Title	Date Completed
Sign off Authority	Angela Van Den	Director of Support Services	

POL00038770

	Bogerd		
Reviewers for Comments and Feedback:	Sandra McBride	SME Network field support	
	Steve Page	TA	
	Sally Rush	TA	
	Gayle Peacock	Product Owner	
	Shirley Hailstones	SME Project Sparrow	
	Angela James	Product Owner	
	Kathryn Alexander	SME Project Sparrow	
	Stefania Ulgiati	SME Remuneration and contract advisor	
	Sharon Rai	SME Security	
	Paul Blackmore	SME Security	
	Chris Hardy	SME Security	
	Joe Connor	Product Owner	
	Dave M King	Information Security Specialist	
	Hector Campbell	SME HR	
	Samantha Williams	SME HR	
Reviewers for Information only	Debbie Ann Young	Virtual HR Specialist	
	Martin Lewis	Project Manager SF	
	Alison Jaap	Owner of TOM	
	Kathryn Lewis	Project manager EUC	
	Kevin Seller	Network Key Accountable Representive	
	Alison Thompson	Transformation Change Key Accountable Representative	
	Mike Fletcher	Communications Key Accountable Representative	
	Matt Keefe	Financial Services Key Accountable Representative	
	Steve Hayes	CIO office Key Accountable Representative	
	Paul Lebeter	Support Services Key Accountable Representative	
	Jamie Butler	Supply Chain Key Accountable Representative	
	Michelle Downs	Commercial Key Accountable	

POL00038770

		Representative	
	Mike Morley-Fletcher	Corporate Services Key Accountable Representative	

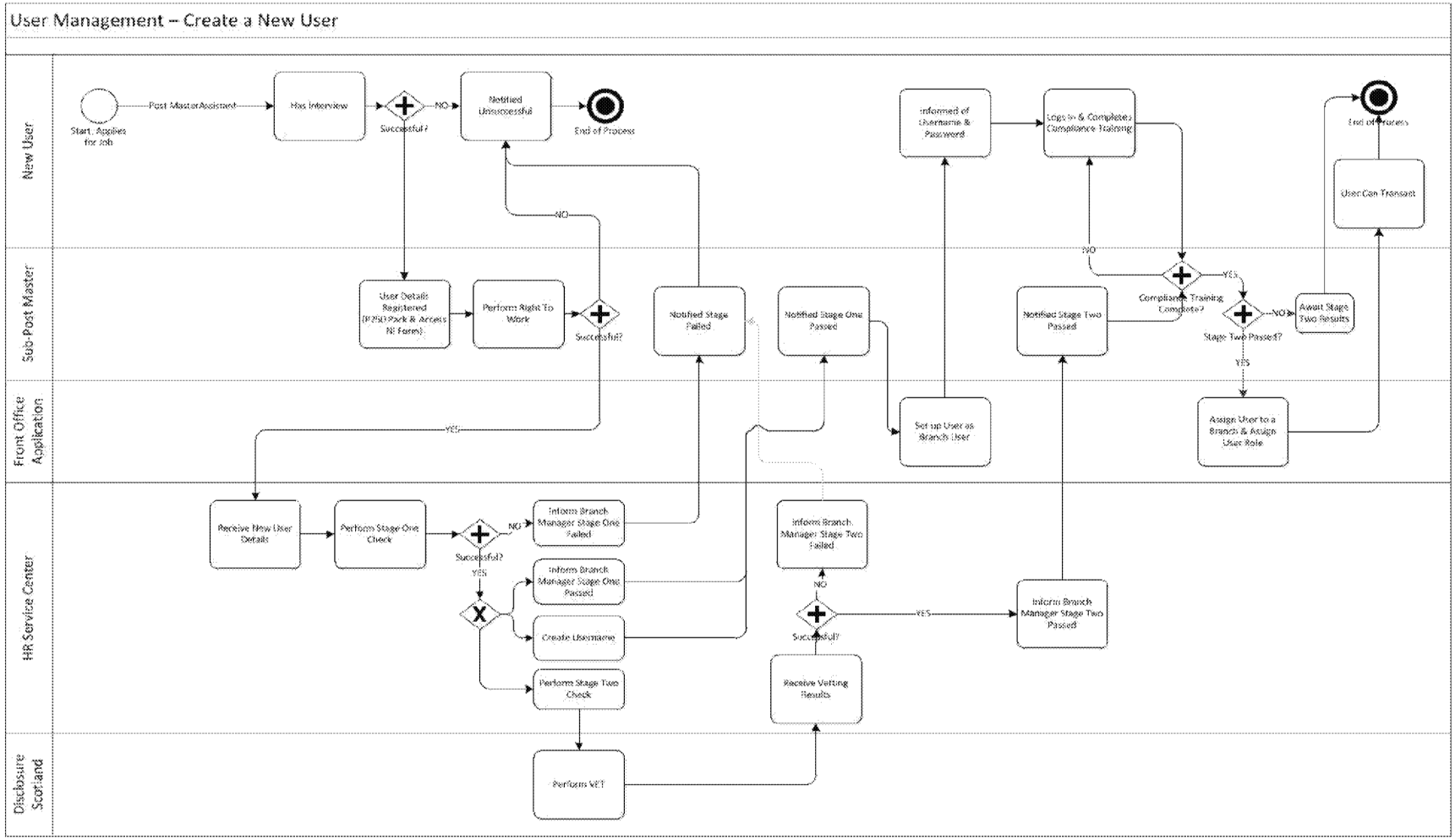
10.3. Referenced Documents

Title	Version	Date	Document Ref.	Location
Global User Process	3.3			
10.11 Enhanced User Management Business Requirements Catalogue	3.0	15.04.16		Embedded
User Management BSD	0.4	21.03.2016		
10.11 Enhanced User Management - Solution options summary	0.3	26.05.2016		
Solution Design Document	0.8	29.7.2016	BTTP_R1_SDD_1_V08@29072016	

POL00038770

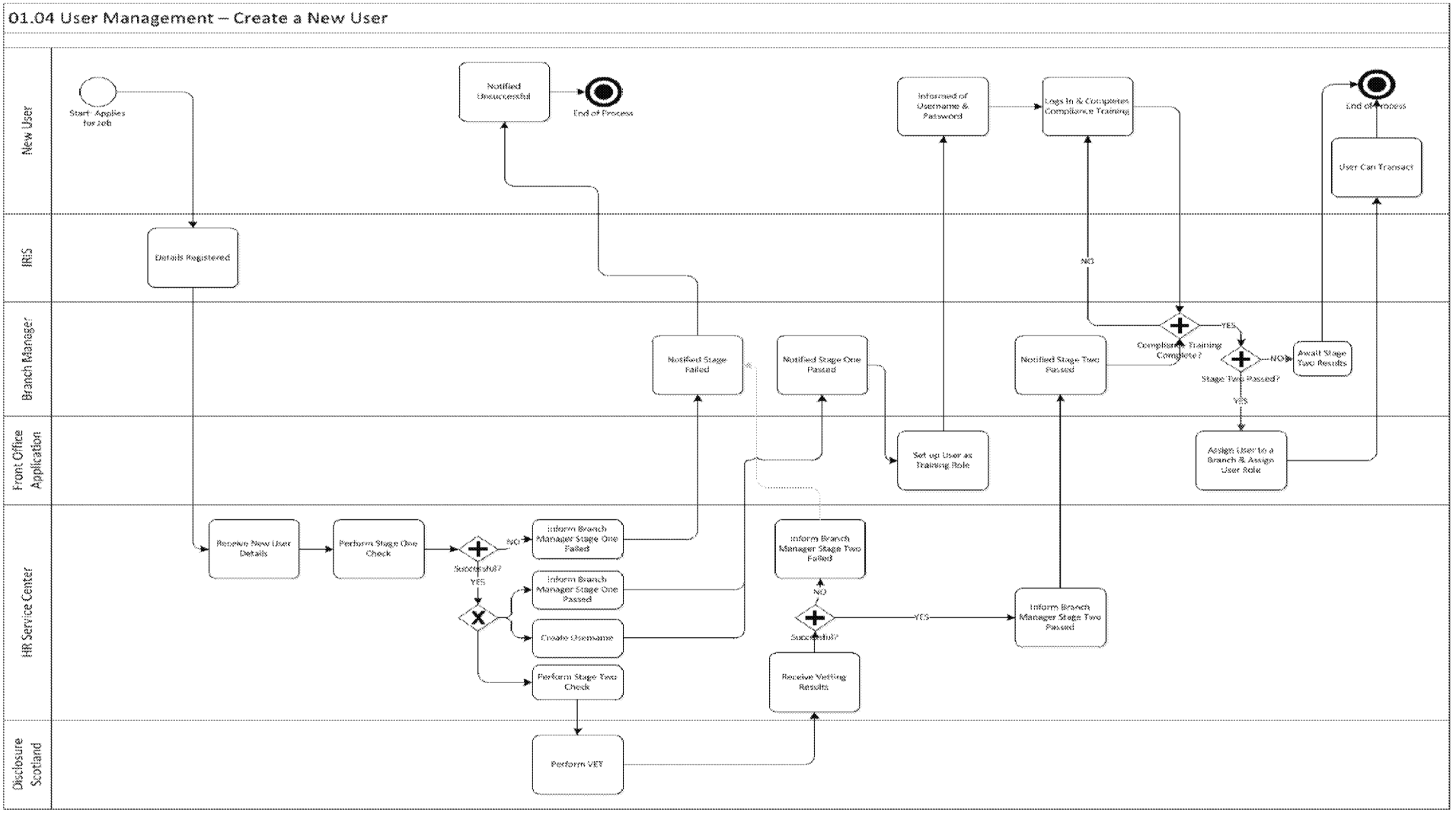
11. Appendix D – AS IS Process Maps

11.1.1.1. Create a New User (Postmaster Colleague)



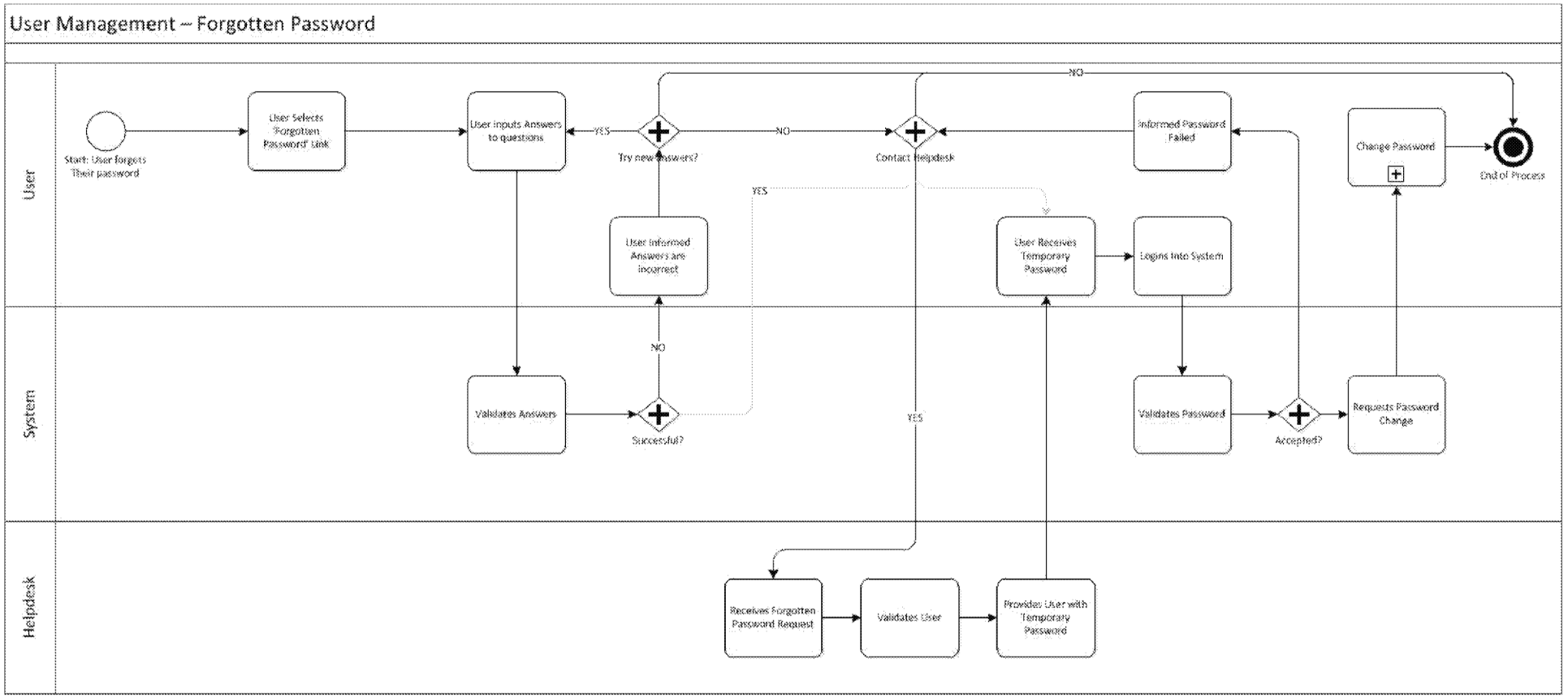
POL00038770

11.1.1.2. Create a New User (POL/Postmaster)



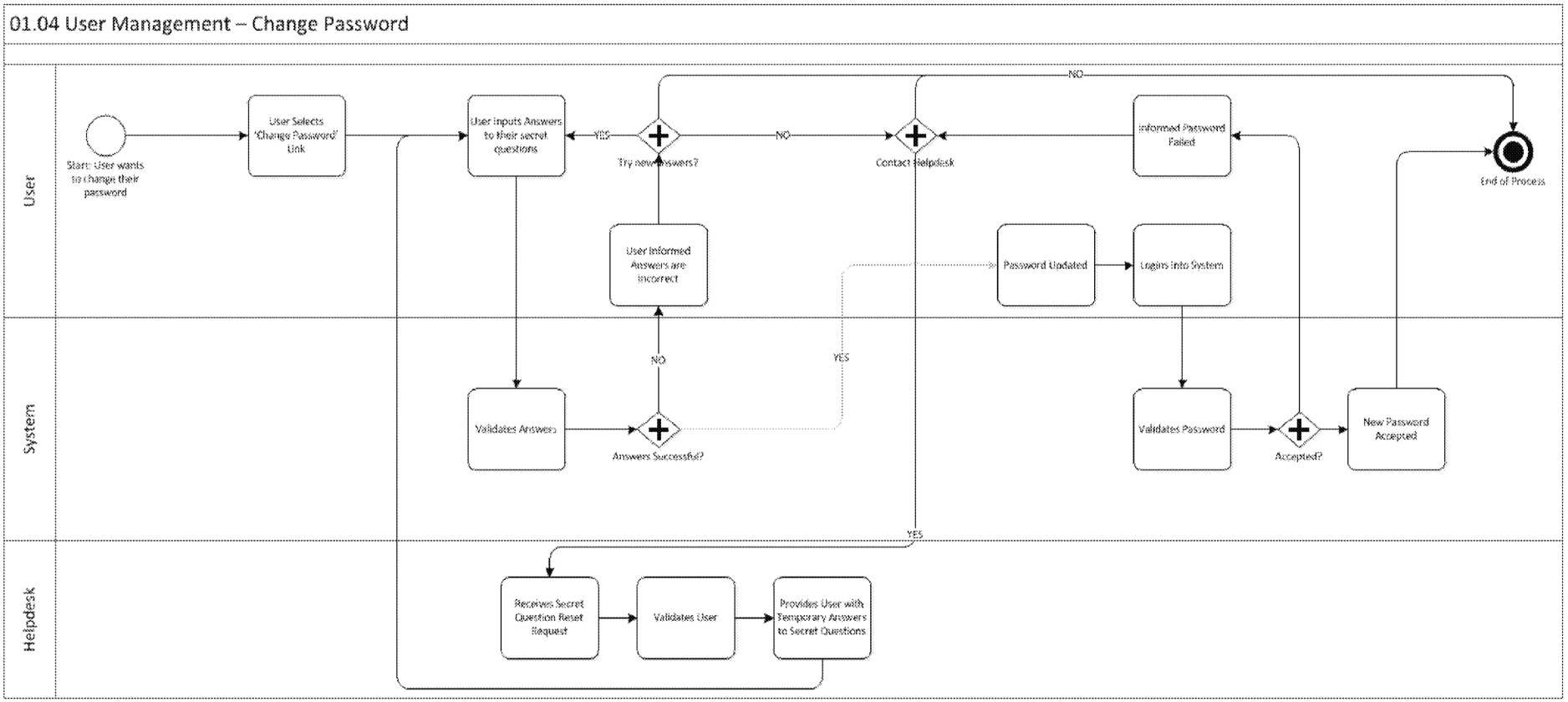
POL00038770

11.1.1.3. Forgotten Password



POL00038770

11.1.1.4. Change/Reset Password



POL00038770

12. Appendix E – TO BE Process Maps

Leavers To Be process maps v1.0.pc