FUJ00232731

POA Improvements – Streams 5-7

Improved Ways of Working & Actions Required

FUJITSU CONFIDENTIAL – INTERNAL USE ONLY (POA ONLY)

Changes in v1.1

1. Split master document to place Streams 5-7 in a separate document
2. Updated Actions

FUJ00232731

POA Improvements – Streams 5-7

Improved Ways of Working & Actions Required

FUJITSU CONFIDENTIAL – INTERNAL USE ONLY (POA ONLY)

Contents

FUJ00232731

POA Improvements – Streams 5-7

Improved Ways of Working & Actions Required

What's New?

This document describes a number of changes to the Post Office Account ways of working and use of systems. This section provides highlights but the entire document should be read to gather awareness of all changes being implemented.

Our interactions needs to be system and process driven, not people and experience – and that will create a clear audit trail too.

We need to limit the dependency on meeting-specific reports or embedded tables in minutes to show progress on important matters.

Transparency is key – to the fullest sensible extent, POL need to see everything – and they need to be able to see it in their systems or from consistent reports from our systems. That way, POL are informed and able to make decisions for us or with us.

FUJ00232731

POA Improvements – Streams 5-7

Improved Ways of Working & Actions Required

FUJITSU CONFIDENTIAL – INTERNAL USE ONLY (POA ONLY)

Introduction & Overview

The Goal…

To implement the defined list of improvements in this document in substantive part by…

31st July 2021

…and to have completed all improvement including any early challenges and snags by

31st August 2021

Purpose & Scope

- By running a series of Streams of work we will systematically drive improvements across POA
- The Streams will likely overlap and may well change format as progress is made
- Although active participation in a Stream may be low for some, it is critical that there is a common understanding or we will not achieve cross functional change
- Stream members may change over time
- Each Stream will have a set of actions to complete – initially derived from this document
- The team can add additional actions as needed
- POA needs to urgently evolve to a cross functionally agreed set of ways of working so that it can be explained to any interested party with ease
- Our interactions needs to be system and process driven not people and experience – and that will create a clear audit trail too
- We need to limit the dependency on meeting-specific reports or embedded tables in minutes to show progress on important matters
- Transparency is key – to the fullest sensible extent, POL need to see everything – and they need to be able to see it in their systems or from consistent reports from our systems. That way, POL are informed and able to make decisions for us or with us
- We need to agree the functions of the various platforms and meetings to ensure it all joins up (this document is a start)
- If POL is tracking it – or applying governance to it – then so should we – and our process should be in advance of theirs so we have no surprises
- We do not have all the tools and integrations we would like, so the goal is to make the best possible use of what we have already
- We need to protect our internal systems from a need for routine disclosure – so we can work our way
- We need to ensure any POL desires on our ways of working relate to contracted obligations and suit how our systems and people work – unless we are commissioned to change any of those – as this is more likely to be consistent and reliable
- For this to succeed we need considerable cross functional support coupled with manager and team member engagement

The Streams

- Stream 5 – Security Improvements
- Stream 6 – Elevated Access & Tooling
- Stream 7 - Various

FUJ00232731

POA Improvements – Streams 5-7

Improved Ways of Working & Actions Required

Each Stream documents the key elements that reinforce an existing way of working or state a new way of working. This content will be embedded into existing account documents for it to be formalised. Each Stream will then contain references to any System Changes made (optional), the One-Time Actions needed to move to the defined ways of working, and then the New Ways of Working that will describe what is different from how things are done today.

Actions that have been completed are scored out. The One-Time Actions that are underway at the moment are highlighted in green although some of the other actions may also be partly active too.

FUJ00232731

POA Improvements – Streams 5-7

Improved Ways of Working & Actions Required

Stream 5 – Security Improvements

- Team – Geoff Baker & Jason Muir

SecOps BAU

- Priority - Geoff
  - Validate PAM roles for Belfast teams. The superuser roles should be the minimum possible to achieve the operational responsibilities
    - DONE
  - Ensure current levels of logging meet MSCF and contract obligations
    - Corporate Confusing
  - Shore up the internal PAM monthly verification processes, and add a report and governance for ISM and CISO review
    - New process, documented, PAM verification good, standard account verification has a few offenders to chase, add to ISMR slides in future
  - All POA users must be reminded that they must follow the account UAM and PAM processes
- TBC
  - Review SVM/SEC/PRO/0012 and check that the 57 RBAC entries are still correct despite it saying last reviewed 19/08/2020
    - FD working on it
  - JML form does not link clearly to ROLE and RBAC
  - Account creation - Wintel & other account creation functions should not use cloning
    - AD (role based in place apart from SOC users as still WIP), Peak (working on it), TfSNow
    - RBAC list accurate, JML form linked, access derived from that
  - Define reports and audience (perhaps all PAM roles) – what do SecOps actually track
  - Define governance to be applied – what do SecOps check is ok and action
  - Update all related documents on UAM and PAM – and contract documents if needed
    - SVM/SEC/PRO/0006 has been retired
  - Look into additional logging, reporting and review of Remote Connectivity activity – or describe 'as is' and seek agreement
    - Now have failed logins in SecOps report from Sept issue

Additional Items

- Priority- Jason
  - ~~Sort/explain non-compliant admin accounts that contravene segregation of duty rules (to EBMS)~~
    - A user account that has admin rights that is used for non-admin activities meaning there could be accidental use of elevated privileges
    - Based on clarification we have none in this category
  - Establish a central register of shared, break-glass and local admin accounts – records of and management of (discovery and processes). Arrange call with Jill Smyth, Andy Gibson, John Bradley, Chris Harrison, Gerald Barnes, Geoff Baker, Andy Hemmingway, Tariq Arain, Matt Swain cc: Steve Bansal, Simon Wilson, Graham Allen
    - Consider…
      - Upgrade KeePass to commercial version/better solution
      - Add KeePass content to weekly report

FUJ00232731

POA Improvements – Streams 5-7

Improved Ways of Working & Actions Required

        - Action
            - Jason has responses from all
            - Automated baseline deployment uses service accounts that are held in BigFix – and there are 200 or so of these
            - Jason trying to catch John Alcock to get ECS support
            - Jason to tell owners there are minimum obligations if they are to retain ownership
    - ~~Confirm meaning of the PCI pen test obligations in the Security Service Description~~
- TBC
    - Investigate the use of the remote Syslog server and determine if any logging should be directed to Netcool. Capacity issues may limit options
        - 23.07

RE Syslog Netcool.msg

        - All of the network (incl. firewall) logs are sent to the Syslog servers. This is good for two reasons: 1) It is best practice to keep your logs off the security platform that may be compromised then it is not easy for the adversary to delete the logs to cover their tracks and 2) Having a central log store makes applying SIEM type intelligence (and doing debugging) easier than having to collect it directly.
        - Netcool was never sized to handle the network logs so it only collects what it considers are “interesting” events. You probably recall that we had similar issues with the Linux and Windows logs under HDCR when we increased the logging to capture forensic detail but Netcool / Tivoli couldn’t cope with the volume. And of course, Post Office have rejected funding a proper SIEM solution.
        - Therefore, we have a lot of network security information in the Syslog servers but it is not monitored or analysed for issues.
        - Action
            - What is “interesting” – John Bradley says it is not documented but is in a baseline
                - We filter out by exception and Jason is waiting for this
                - Need to check this doesn’t exclude things we want to cover
                - What’s we keep goes to Netcool and to Audit Archive
            - How long do we keep the syslog events for?
                - Forever if in Audit Archive
    - Counter access – why are counters accessed so frequently, should access be on request not by default to protect our staff and the company from incorrect accusations.
        - Action
            - We need to restrict RCA capability to escalate privileges
            - We need to confirm that RCA commands are read only
            - We need to confirm with CC that the user account on the counter are read only
                - All documented in DES/GEN/SPE/2745

FUJ00232731

POA Improvements – Streams 5-7

Improved Ways of Working & Actions Required

FUJITSU CONFIDENTIAL – INTERNAL USE ONLY (POA ONLY)

Actions

System Changes

- TBC

One-Time Actions

Priority

1. **Geoff** - Challenge and reduce Belfast admin rights to sensible minimum
    a. Belfast teams creating new granular specific admin roles and assigning team to more specific responsibilities. Impact has been a reduction of admin rights from 56 to 34. Implemented monthly (weekly) verification
    b. DONE
2. **Geoff** – Create an action plan to address all MSCF gap findings
    a. Mapping complete. Chasing validation from corporate and then we can identify the actions we need to consider
    b. SB wrote to Keith Barnes for clarity
    c. GB still waiting for feedback
    d. Obvious get well gaps should be done - GB
3. **Geoff** – Review and improve monthly PAM verification process and ensure fully documented. Include the proposed Belfast team checks sent to Andy and Jill too
    a. POAUSERMANAGEMENT responses will be built into the process
    b. First checkpoint meeting 23/8 – then update 0012
    c. Needs to be all PAM roles not just AD ones – TACACS, TESQA, Room access
    d. There will be a document we can review – 0012 probably
4. ~~**Steve** – Issue a Red Top reminding POA users to use the account UAM and PAM processes. Sent by Red Top 18.06.2021~~
5. **Jason** – confirm any POA admin account anomalies to EBMS and either document reason or amend privileges
6. **Jason** – Conduct discovery and collation activity to get the full list of all local admin type accounts
    a. Underway and due to complete in a week or so
7. ~~**Jason/Steve** – confirm understanding of PCI pen testing obligations.~~
    a. ~~These must be initiated by POL so no further action required~~

New Ways of Working

1. **Geoff** – PAM verification process to be reported on monthly within SecOps governance (to include routine validation of superuser roles)
2. **Geoff** – operate the monthly PAM verification process to a higher-level of rigour
3. **SecOps** – Maintain records of all shared/service/local admin accounts and spot check the processes around them

FUJ00232731

POA Improvements – Streams 5-7

Improved Ways of Working & Actions Required

Stream 6 – Elevated Access & Tooling

- Team – Varied. Mostly a one-time action stream

Actions

One-Time Actions

APPSUP

1. **Sandie** – Complete updated APPSUP process document and get all Fujitsu teams to overtly confirm compliance
2. **Adam –** Ensure 4 eyes/peer review happens - NWH or OOH
3. **Steve Br –** Amend both organisations' Change Control documents to show APPSUP is allowed out of process

APPSUP – non-BRDB

1. **Geoff** – Revoke default privileges once impact quantified
2. **Sandie/Adam –** Update APPSUP document to incorporate findings and changes
3. **Steve Br –** Notify POL of action taken

Interface Interactions Logging

1. ~~**Steve Br/Wendy** – Confirm with POL that this must be Fujitsu support use only – not for sharing~~

Transaction Correction Tool

1. ~~**Steve Br/Seb** - Decommission TC Tool functionality as not used. Completed 14.05.2021~~

FUJ00232731

POA Improvements – Streams 5-7

Improved Ways of Working & Actions Required

Stream 7 – Various

- Team – Varied. Mostly a one-time action stream

Actions

One-Time Actions

Historical Investigations

1. **Steve Br** – We must log them and manage this differently – we need a process defining internally and with POL
2. ~~**Steve Br** – TfSNow and Peak teams must intercept them and not action but divert to the process~~
3. **Steve Br** – All staff must realise the need to demand a TfSNow ticket is raised by POL (hence the above intercept will apply) – it cannot come in via email only

Monthly SMR pack

1. **Steve Ba/Sandie** – Limited Incident data - add trending and patterns
2. **Steve Ba/Sandie** – Highlights page is largely of no value
3. **Steve Ba/Sandie** – Some cumulative failures are not carried forward in stats columns
4. **Steve Ba/Sandie** – We embed minutes of other meetings and list Incidents - it's overly padded
5. **Steve Ba/Sandie** – Needs to add links to HDR Defects

Peripheral Key Logger

1. **Steve Br** – Decommission functionality as not used
    - Steve Browell asked Dean Bessell again on Thursday 24th June 2021 to check with Lorna Owens and get us a decision. CBIF 12.07.2021 has shown some POL confusion that will be addressed at CBIF 19.07.2021
    - This is progressing under FOC CWO and will likely be in the next counter release in 2022Q1

Documentation

1. **Steve Br/Matt L** – We need to get all fundamental content gaps identified and actions assigned
    - Outstanding CCD actions
    - Service Descriptions
    - Referenced documents in the contract
2. **Steve Br/Matt L** – Document list:
    a) Security Service Description SVM/SDM/SD/0017
    b) Governance Schedule A2 – names, chair and scope of meetings
    c) ASM Schedule I2 – BIF definition, Peak and KB proprietary references, POL KB references for approved BEDs
    d) Testing Strategy - 0936 document
    e) REQ/GEN/PRO/0735 – new CCD with Steve Evans to complete
    f) The CBA document Simon mentioned had the wrong Windows version in it
    g) SVM/SDM/SD/0003 – DC Ops SD – states plans we should be creating [looks to be ok – Steve Br to double check]
    h) Change Control to mention APPSUP
    i) Application Support Strategy to mention Peak and Live Defect Management

FUJ00232731

POA Improvements – Streams 5-7

Improved Ways of Working & Actions Required

FUJITSU CONFIDENTIAL – INTERNAL USE ONLY (POA ONLY)

Governance Meetings

1. **Steve Br/Dan –** The contract Schedule A2 needs updating
2. **Steve Br/Dan –** Key Meetings must have a Chair, ToR, Agenda, Minutes, correct attendance
3. **Steve Br/Dan –** Working list of key meetings (POL attempting to lead on this):
    a) Governance Meeting (Supplier Meeting)
    b) Demand Planning
    c) RAM/RAB
    d) Change Control