FUJ00080630

Security Assessment	Ref: LOC/CSO/Privilege Management /PostOffice/220413 Issue:1.0 Date:26/07/2013

Assessment Control Page

Assessment Type	Internal	**Assessment Reference**	Ref: LOC/CSO/Privilege Management /PostOffice/22042013
Area	HNS	**Processes Assessed**	Privilege Management
Contact(s)	Brad Warren	**Process Owner(s)**	Deborah Haworth
Planned Date	11/04/2013	**Lead Assessor**	Gurbir Singh
Start Date	11/04/2013	**Full Report Title**	PostOffice Privilege Management Assessment Report

Assessment Summary

1. Objective of Assessment

Undertake an internal security review of the above unit and assess local privilege management processes and working practice including:

Whether the Account is responsible for privileged account management, or has privileged accounts, in the following areas:

- Domain administration;
- Servers;
- Firewalls;
- Networks;
- Applications;
- Any others.

Where devices and/or systems are managed centrally or there is no privileged access then the assessment will not be applicable.

FUJ00080630

Each technology area will be checked to ensure:

- Privileged accounts are identified;
- The principle of least privilege is recognised and implemented;
- The Delivery Exec has accepted accountability for the use of privileged access across the Account;
- Actions are being taken to minimise the number of privileged accounts;
- A documented process is in place that contains the process steps in the high level process flow produced by the office of the CSO;
- Regular reporting is being produced which contains the elements listed in the Process notes produced by the office of the CSO.

There will also be a check that the regular communications from the Fujitsu UK&I CSO on this topic are being cascaded appropriately.

2. Scope of Assessment

Function / Role	**Interviewee**
CSO	Brad Warren
Security Operations Manager - Post Office Account	Donna Munro
POA BU Quality & Compliance Manager	Bill Membery
Security Operations team	Kumudu Amaratunga
Crypto Key Manager	Andy Dunks
Security Operations	Rajbinder Bains

FUJ00080630

3. Management Summary

During this Assessment a total of: 1 Non-**conformances**, 1 **Observations** and 0 **Good Practice Observations** were raised.

Operations Overview

Findings are limited to the areas sampled during this visit. The context of the findings is described in the commentary below. In summary, the main findings and recommendations are as follows:

No	Category	Finding	Recommendation	Actionee	Completion date
1	Obs	The details of the fields held within this user register are shown in Appendix B of the procedure but states that "this is not a exhaustive list".	It is recommended that the user registration process exhaustively specifies every PO systems that the account manages access for. The Privileged Access Process notes produced by the office of the CSO may help.	CISO	11/11/2013
2	Obs	It was noted that this procedure (SVM/SEC/PRO/0012) was last reviewed in October 2011.	It is recommended that this procedure is reviewed and reviewed at least annually thereafter.	CISO	11/11/2013
3	Obs	The document "The Post Office Account User Management LWI", first produced in 2011 is still in draft.	It is recommended that this document is reviewed, approved and published.	CISO	11/11/2013
4	NC	Neither the user access procedure nor the associated work instruction lists the matrix of privileges associated with the PO systems that users can potentially request.	It is recommended that a matrix is established listing all of the PO systems along with possible privileges that user accounts may have.	CISO	11/11/2013
5	NC	There is no documented procedure on how to process a request for a privileged account in an emergency situation.	It is recommended that a section is added within the user registration process that describes how a request for a privileged user accounts should be processed.	CISO	11/11/2013

FUJ00080630

6	NC	The User Registration Procedure lists references to several corporate documents but the mandatory Security Master Policy and the notes associated with privileged access user notes are not.	It is recommended that the user registration process and the associated work instructions incorporate references to both the Security Master Policy and Privilege Access requirements.	CISO	11/11/2013

Please see Appendix I for details of observation categories

FUJ00080630

4. Assessment Commentary

4.1 Technology Status

Following this assessment the technologies have been RAG coded as follows:

Domain Admin	Server Admin	Firewall	Network	Applications	Other Admin

Firewalls are provided centrally as a managed service and are therefore not applicable to this assessment.

Networks are provided centrally as a managed service and are therefore not applicable to this assessment. However, the PO security operations team manage the encryption keys used over the WAN links, no additional privileged accounts are associated with this activity.

A Fujitsu global team based in India provides development and support for the primary application Horizon Next Generation (HNG-X) application. Privileged accounts used by that team are subject to the "POA User Access Procedure.doc".

Domain and server administration is provided by a dedicated Wintel support team.

Other privileged accounts are used by contractors, third parties, Oracle, DBA, SAP and non POA Fujitsu staff is subject to the user registration process.

4.2 Key Principles and Accountability

The PO account is large and has an appropriately large security team. It is clear that the DE was aware that he is accountable for the for privilege access across the account.

Access Control procedures should be consistent with the Access Management guidelines on page 4 of the Minimum Security Control document available here.

A new CISO has been recently appointed to this account. Additional key positions within the security team have been filled but some remain vacant. A service improvement plan was established in late 2012 ahead of a BV external audit. The external auditor was satisfied with the plan and the audit concluded with a single non-security related finding.

4.3 Process Control

This is a large account requiring the support of several internal capability units. A user account database is maintained which includes details of the privilege account. Authorisation for the privileged access is provided each user's manager. TfS is used to record all user access requests.

There are two documents associated with user registration

FUJ00080630

The main procedure "POA Usser Access Procedure.doc - SVM/SEC/PRO/0012" and an associated work instruction "The Post Office Account User Management LWI" which does not have a document reference at this time.
The user register holds details about each user, the nature of the access and the system they have access to. In addition it contains details of the authoriser, approver and dates that this access was granted, last reviewed and revoked.

#1 Observation
The details of the fields held within this user register are shown in Appendix B of the procedure but states that "this is not a exhaustive list". It is recommended that the user registration process exhaustively specifies every PO systems that the account manages access for. The Privileged Access Process notes produced by the office of the CSO may help.

#2 Observation
It was noted that this procedure (SVM/SEC/PRO/0012) was last reviewed in October 2011. It is recommended that this procedure is reviewed and reviewed at least annually thereafter.

A work instruction associated with the User Registration Procedure called "The Post Office Account User Management LWI" appears not to be a formal document. It was first produced in 2011 and is still in draft.

#3 Observation
The document "The Post Office Account User Management LWI", first produced in 2011 is still in draft. It is recommended that this document is reviewed, approved and published.

The security operation manager confirmed that each privilege access request is verified monthly via an email to the team manager of the account holder. Third Party (including off shore) engineers as well as SAP and DBA access are subject to the user registration process.

During the review the operational security manager confirmed that the user registration process is integrated with the Joiners, Mover and Leavers process.

The operational security team is responsible for issuing and audit of the two factor authentication used by system administrators.

Section 2.1 of the User Registration process links the revocation with the leavers' process.

#4 Non Conformance
Neither the user access procedure nor the associated work instruction lists the matrix of privileges associated with the PO systems that users can potentially request. It is recommended that a matrix is established listing all of the PO systems along with possible privileges that user accounts may have.

4.4 Process Reporting
Recently published guidelines require that privileged accounts are monitored and regularly reviewed. During the review the operational security team indicated that a regular monthly review of accounts with privilege access was in place.

FUJ00080630

A recent external report (Fujitsu-Post Office ISAE3402 Report - 1 April 2012 to 31 December 2012) confirmed that the principle of "Least Privilege" was implemented in the user creation and management process. However, the term "Least Privilege" is not used in the User Registration process or the associated work instruction.
Section 5.1 of the User registration states the following regular reporting associated with processing of user account requests

- access rights and roles with each functional area is carried out on a biannual basis as minimum and will report findings in the Operational Security monthly dashboard
- all human (i.e. exclude system) accounts that have been unused for a period of 90 days will be disabled and the line manager contacted
- a monthly report detailing all joiners, leavers and movers on the account from RIOs and ERICs.
- reports are reviewed jointly with PO Ltd at the regular Information Security Management Forum (ISMF)

The process User Registration process clearly integrates the requester's line manager, Fujitsu HR Joiners & Leavers process and the PO operational security team that provide user access.

4.5 Ongoing Communication
The CISO confirmed that the DE is receiving and cascading the regular communications from the Fujitsu UK&I CSO on the management of privilege accounts. The Fujitsu CISO and customer CISO meet at least during the regular ISMF meetings but staff changes on both sides has introduced a temporary break in the regularity of these meetings.

Although it is likely to be a rare request, there is no procedure to guide a request for the creation of a privileged account in an emergency.

#5 Non Conformance
There is no documented procedure on how to process a request for a privileged account in an emergency situation.It is recommended that a section is added within the user registration process that describes how a request for a privileged user accounts should be processed.

During the review it was evident that the account team was aware of the issues associated with the privileged level access. The following resources should be useful in the document review and the establishment of the recommended user registration process.

#6 Non Conformance
The User Registration Procedure lists references to several corporate documents but the mandatory Security Master Policy and the notes associated with privileged access user notes are not. It is recommended that the user registration process and the associated work instructions incorporate references to both the Security Master Policy and Privilege Access requirements.

The following links should be of use.

- New Security Portal

FUJ00080630

- Security Master Policy
- Security Policy Manual PDF
- Privilege Access Requirement
- Privileged Account process flow and Process notes produced by the office of the CSO.

Appendix I – Observation categories

In terms of the Assessment Database, *observations* fall into 3 categories:

- **Non-Conformance**:
  - *Definition:* No evidence that documented policy, minimum controls or mandatory process are being met.
- **Observation:**
  - *Definition:* A business observation, usually made where substantial elements of the requirements of the privilege management process are being met but there are clear opportunities for improvement.
- **Good Practice:**
  - *Definition:* A specific local process or general working practice, or the implementation of a Corporate Process in such a way that it is regarded as being good practice, over and above expected implementation, and worthy of adoption by other parts of Fujitsu.