FUJ00080645

Security Assessment

Ref: GHQ/SEC/BAS-Apt Services /UKI-Skype/290317
Issue: 0.1
Date: 20th April 2017

Assessment Control Page

Assessment Type	Internal	**Assessment Reference**	Ref: GHQ/SEC/BAS-Apt Services /UKI-Skype/290317
Area	BAS –SEC-Apt Services	**Processes Assessed**	Privilege Management
Contact(s)	Gary Huteson	**Process Owner(s)**	Deborah Haworth
Planned Date	29th March 2017	**Lead Assessor**	Margaret Thomas
Start Date	29th March 2017	**Full Report Title**	Apt Services PAM Report

Assessment Summary

1. Objectives 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.

Each technology area will be checked to ensure:

FUJ00080645

- 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 Security Governance team;
- Regular reporting is being produced which contains the elements listed in the Process notes produced by the office of the Security Governance team.

2. Scope of Assessment

This Fujitsu Services Internal Assessment was conducted on Skype and involved the following employees:-

Function / Role	Interviewee
Apt Methods and Tools - Operations Manager	Gary Huteson

FUJ00080645

3. Management Summary1

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

Reference / Sequence	See table below	**Date of Observation**	26/09/16	
Category	See table below	**Standards / Section**	ISO 27001	See table below for each finding
Corporate Process	Security Policy Manual (Impact see table below)	**Local Process**	See MSCF reference in table below	
Unit	BAS-SEC-Apt Services	**Country**	UK	
Location	SkyPe	**Division**	BAS	
Interviewee	See table below	**Interviewee's Role**	See table below	
Area Contact	Deborah Haworth	**Assessor's Name**	Deborah Haworth	

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	Cat.	27001/ MSCF	Finding	Recommendation	Interviewee Name and Role	Actionees Name	Completion by date	Impact Minor Moderate Major
1								

Please see Appendix I for details of observation categories

FUJ00080645

4. Assessment Commentary

Apt provides industrialised methods and tools that enable Fujitsu project and account teams to deliver services to our customers in an efficient, collaborative, consistent and repeatable way. These tools are fully integrated to provide automation of the project lifecycle and method.
Specialised support and tools are provided for different endeavours such as Managed Service, Application Integration, Infrastructure Delivery, Prototyping, Mobile Development etc. Appropriate methods and tools can be selected to meet specific delivery requirements.
Apt cloud services are delivered as fully managed, hosted, secure and 'ready to use' environments consisting of automated processes and integrated methods and tools.

The service is hosted on local cloud at SDC01and managed by the GDC, Kazan, Russia. Each project has its own SharePoint site and no personal data is held. Awareness is delivered by the Operations Manager to everyone who is given access.

4.1 Technology Status

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

Domain Admin	Server Admin	Firewall	Network	Applications	Other Admin

4.2 Key Principles and Accountability

The Apt Methods and Tools Programme Manager accepts accountability for PAM and is the approver for all access requests.

4.3 Process Control

The Apt Services Privileged Access Register spreadsheet is the register of the various elements supporting the Apt Team's approach to Privileged Access Management and is maintained on an ongoing basis and is reviewed each month at the Apt Monthly Service review.

The register details access level for each use and includes removed users as below:-

System Admins	Level of access equal to admin account, e.g. almost everything
User Admins	Accessing Crowd/BOS and User Management
Apt Core Admins	full access and configuration of Apt internal areas at JIRA, Confluence etc

There is a worksheet that shows Logs of Admin Password Changes which should have been completed in March but is showing as postponed until the “Bitbucket Accessor” change has been implemented. Task APTMGNT 307 has been raised as one tool still needs to be updated so that Bitbucket Accessor can be fully implemented.

KeePass is used by the Core Apt, NI Support and Apt GDC Teams to store and manage passwords. The Operations Manager changes the password monthly. Users do not store privileged access passwords using a browser's 'Saved Logins' feature.

The Apt Local Security Procedure outlines the PAM Process Mapping

FUJ00080645

SCOPE

- OpenSource Shared Service Administrator Usage
- OpenSource Apt Core Internal Access
- OpenSource Vendor Licenses
- Microsoft Service Administration
- Apt SharePoint Portal Owners
- Apt SharePoint Contributors

1. Privileged Account Creation (New Joiners and New Privileged access requests)
    - Requests for Privileged Access (Administrator Password etc) are raised via email with the Apt Service Manager by the Security Officer
        - Requests should be raised with the Security Officer via the Apt Deployment mailbox
        - Approvals are actioned by the Apt Security Officer
        - Approvals are logged in the register of privileged access
        - Rejections are logged in the register of privileged access
2. Privileged Account Management
    - Privileged Account Access is reviewed monthly by the Apt Service Manager and the Apt Security Officer at the Apt Service
        - Review.
        - Review covers all the element in Scope (above)
        - Leavers, Access Renewals, Revocations and Accounts not used
        - Register of privileged access is updated
    - OpenSource Administrator password is :-
        - Changed, at a minimum, on a monthly basis - by Apt Security Officer
        - Changed when an administrator password holder leaves the Team - by Apt Security Officer
    - OpenSource Software Licenses
        - Password protected spreadsheet in use
        - Password changed on a monthly basis - by Apt Security Officer
        - Password changed should the Apt PCO or Security Officer leave the team - by Apt Security Officer
    - Access Revocations
        - Revocation of Privileged Access are raised via email with the Apt Service Manager
        - Revocations are actioned by the Apt Security Officer
        - Revocations are logged in the privileged access register.
3. Privileged Account Reporting
    - The privileged access register contains all privileged users for each of the areas in Scope
    - Privileged access register is reviewed on a Monthly basis

Privileged Account Access is reviewed monthly by the Apt Service Manager and the Apt Security Officer at the Apt Service to ensure the right level of access is in place and the access is still needed.

FUJ00080645

Five members of the NI Support team have User Admin Access but do not have System Admin Access. As the NI Support team are a shared service the accounts are not revoked when not used but the access list is reviewed by the Operations Manager monthly.

A reminder is sent to change passwords every month as an extra precaution since the March 2017 security incident.

Example shown with email to the Apt Methods and Tools Programme Manager, and his response with the following question
Is there a plan to ensure that this employee is aware of our local security procedures?
The log in the register shows that the example user was given access on 13/12/16 and received the Security Awareness on the 14/12/16.

Requests once approved are controlled by MIS. GDC Russia have 20 users who have high level access to make changes following a request via TfS from the Apt Services team.

The Apt Team Changes Checklist details changes required to the various Apt teams and supporting functions when membership of the Apt Support and/or Apt Development teams change.

What Needs to Change?

- Apt Server Access
- Triole for Services Service Desk Access
- Apt Team Changes Attachments

The checklist includes the process for Joiners and Leavers of all the different teams detailing the naming convention which is linked to access given and shown in the register.

Apt Server Access
For new support team members who will be supporting the Apt for Java Service access to the live servers ASAPTLCP01,
ASAPTLCP02 and ASAPTLCP03will be required. This is done by the MIS GDC teams and is arranged via a TfS Change Order.

TfS Service Desk Access
When there are Apt Support Team joiners or leavers access to the Java and .NET Support resolver groups needs to be revised. This is actioned by the NI Support Team Manager.

No emergency access process is required as it is a shared service.

4.4 Process Reporting
The privileged access register contains all privileged users for each of the areas in Scope
Privileged access register is reviewed on a Monthly basis at the Apt Monthly Service Review.

FUJ00080645

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.