



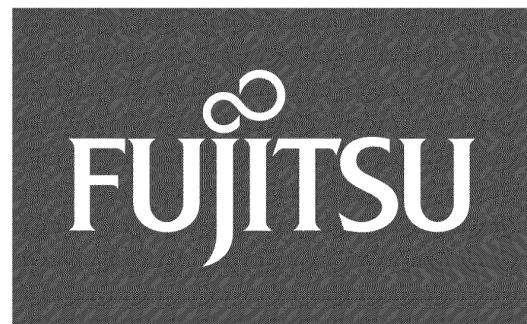
Move Forward with Confidence



Bureau Veritas Certification

External Assessment Report

UKGBD – CGBU –EEE – BIS Account



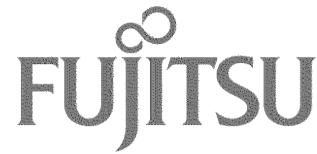
Report Number: EXT/BV/Post Office Account/BRA01/311013

Office Account/BRA01/311013 Unit/LOC/Conn/DD/MM/YY

Bureau Veritas External Assessment of the Post Office Account and associated Service Line
delivery capabilities.



Move Forward with Confidence



MANAGEMENT SUMMARY

During this Assessment of the Post Office Account a single Observation relating to Security awareness training was raised.

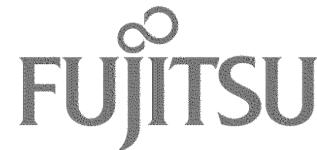
In summary, the main findings were as follows:

- Overall implementation of BMS policies / processes operational control and understanding of objectives was found to be good with appropriate levels of communication and review in place.
- Several examples of compliance with BMS policies and processes were in evidence as well as alignment between local procedures and BMS processes.
- **OBS:** Staff may not have received appropriate awareness training and regular updates in organisational policies and procedures as Corporate security training was last provided about 18 months ago.

Continued certification to ISO 9001:2008 and ISO 27001:2005 is recommended.



Move Forward with Confidence



MANAGEMENT SUMMARY.....	2
1. ASSESSMENT CONTROL.....	4
2. OBJECTIVES OF THIS ASSESSMENT.....	4
2.1 OBJECTIVES.....	4
3. SCOPE.....	5
3.1 INTERVIEWEES.....	5
3.2 ASSESSMENT SAMPLING.....	5
4. ASSESSMENT COMMENTARY.....	6
4.1 ACCOUNT OVERVIEW, REGIONAL ACCOUNT BUSINESS PLAN REVIEW, CUSTOMER SATISFACTION, CORRECTIVE ACTION – HAYDN JONES, GAVIN BELL, MARK ARNOLD.....	6
4.2 PROGRAMME & PROJECT MANAGEMENT – BRIAN McCANN.....	6
4.3 INFRASTRUCTURE SOLUTIONS DESIGN AND DEVELOPMENT (IDBM) – ANDY HEMINGWAY, TIMOTHY SALISBURY, DAVE IBBETT.....	7
4.4 <i>BMS, INTERNAL AUDIT, CORRECTIVE ACTION, CONTINUAL IMPROVEMENT, QUALITY AND SECURITY MANAGEMENT REVIEW, PERFORMANCE DASHBOARD, PHYSICAL AND ENVIRONMENTAL SECURITY – BILL MEMBERY, NENEH LOWTHER.....</i>	7
4.5 IMPLEMENTATION & TEST SERVICES – MARK ASCOT.....	8
4.6 SECURITY DOCUMENTATION AND MANAGEMENT FUNCTIONS, SECURITY HEALTH CHECKS, ISMS IMPROVEMENT, INFORMATION SECURITY INCIDENT MANAGEMENT – TOM LILYWHITE, KUMUDU AMARATUNGA, CHRIS COLE, DAVE HAYWOOD.....	9
4.7 APPLICATIONS SOLUTIONS DESIGN AND DEVELOPMENT – NICK LAWMAN.....	10
4.8 APPLICATION IMPLEMENTATION AND SUPPORT – STEVE PARKER.....	10
4.9 CHANGE CONTROL – ALAN FLACK.....	11
4.10 SERVICE DESK, OPERATIONAL BUSINESS CHANGE, SERVICE MANAGEMENT, MONITORING AND REPORTING – LEIGHTON MACHIN, SANDIE BOTHICK, MARK JONES.....	11
4.11 DATA CENTRE DELIVERY, PLANNED PREVENTIVE MAINTENANCE, BUSINESS CONTINUITY TESTING – JOHN HILL.	12
4.12 FINANCE MANAGEMENT REPORTING – MATTHEW CHURCH.....	12
5. OBSERVATION.....	13
5.1 OBSERVATION REF.1.....	13



Move Forward with Confidence



1. ASSESSMENT CONTROL

Assessment Type	External	Assessment Reference	EXT/BV/POST OFFICE ACCOUNT/BRA01/311013
Area	Post Office Account	Processes Assessed	Various (See Scope of Assessment)
Contact(s)	Bill Membery	Process Owner(s)	Various (See Scope of Assessment)
Planned Date	31/10/13	Lead Assessor	Paul Bonnet
Start Date	31/10/13	Issue	0.2

2. OBJECTIVES OF THIS ASSESSMENT

2.1 Objectives

This Bureau Veritas External Assessment focused on key business functions performed within the Post Office Account and associated Service Line delivery capabilities, and considered, through the assessment of local processes and working practice:

- The compliance of those functions with relevant aspects of the ISO 9001, ISO 27001, and any other applicable standards.
- The compliance of those functions with the Fujitsu UK & Ireland Business Management System (BMS).
- Any areas suitable for promotion as good business practice, in relation to meeting the requirements of the standards being assessed against, across Fujitsu UK & Ireland.



Move Forward with Confidence



3. SCOPE

This Bureau Veritas External Assessment concentrated on the Post Office Account, and was conducted over 2 days, within the customer's BRA01 site and involved the following members of staff:

3.1 Interviewees

Function / Role	Interviewee
Client Managing Director (by teleconference)	Hadyn Jones
Client Executive	Gavin Bell
Head of Business Management	Mark Arnold
Programme Manager	Brian McCann
Service Manager	Andy Hemingway
Senior Project Manager	Timothy Salisbury
Infrastructure Deployment Manager	Dave Ibbett
Quality Manager	Bill Membery
Quality, Audit and Compliance - Post Office Account	Neneh Lowther
Test Manager	Mark Ascot
CISO	Tom Lillywhite
Security Operations Manager	Kumudu Amaratunga
Senior Security Consultant	Chris Cole
Security Architect	Dave Haywood
Software Development Manager	Nick Lawman
Managed Services Strategic Support Lead	Steve Parker
Operational Change & Release Manager	Alan Flack
Lead SDM	Leighton Machin
Service Delivery Manager	Sandie Bothick
MI Systems Lead	Mark Jones
Data Centre Manager (WEBEX audit session)	John Hill
Financial Controller	Matthew Church
Assessment Guide	Bill Membery

3.2 Assessment Sampling

The assessment was based on random samples and therefore non-conformities may exist which have not been identified. Audit findings raised are categorised as Non-conformities and Observations.

The following issues and areas have been identified for follow-up during future Surveillance Visit:

- Amber Alert raised relating to a SAP weekend release that did not go to plan and required resolution with SAP
- Once all risks, threat and plans completed, then controls are to be identified to contain the live and residual risks identified by the STREAM Risk Management Tool
- Service Desk activities in Stevenage
- Release 9 Project activities
- Business Change Control (generated by customer)
- Q2 2014 internal audit of the management of 4th line Application Support provided by the Fujitsu GDC team in India



Move Forward with Confidence



4. ASSESSMENT COMMENTARY

4.1 Account overview, Regional Account Business Plan Review, Customer Satisfaction, Corrective action – Haydn Jones, Gavin Bell, Mark Arnold

Assessment Evidence: Account review PowerPoint Presentation slide deck dated 2/7/13, Meeting 2nd July 2013 – Regional Account Business Plan Review, CSIP Action Plan 2012 V12, CSIP Action Plan 2013 V4

- An overview of the Post Office Account was provided as follows:
 - Major UKI Fujitsu Account with Horizon System developed and supported by Fujitsu
 - Around 11,500 locations contain approximately 30,000 end points such as PCs, scales, pin Pads, printers
 - Post Office is undertaking a network transformation in partnership with Fujitsu
 - Current contract to March 2015 with recently awarded extension to March 2017
- Input to biannual Account Review of Account Plan seen to include Service Overview of performance against contractual SLA targets (both met), Strategy On A Page (SOAP) and quarterly review of MTP.
- Output of this Regional Account Business Plan Review seen to include actions with due date, updates highlighted in red text, with details of how actions completed.
- CSIP figures for 2013 to date are between 8 and 9. All actions from 2012 CSIP Action Plan seen complete. CSIP Action Plan from January 2013 interview seen to include status updates column with dated updates and details for closed actions.

4.2 Programme & Project Management – Brian McCann

Assessment Evidence: Post Office Account Demand Planning Forum slide pack, Joint Programme Board slide pack, Demand Planning Forum and Joint Programme Board Minutes – Meeting No. 44 dated 22/4/13, Weekly Project Progress Report dated 18/10/13, Issues Log

- It was explained that Release 9 of the Horizon Next Generation (HNG-X) consisted of 5 projects which followed the Delivery Lifecycle described on the POA Programme Portal which includes;
 - Change Request received from Client
 - Change Proposal drafted by Fujitsu
 - Contract Terms and approval by Client
- Monthly Joint Programme Board Meeting held with Client to review Risk Register and Issues Log
- A list of Project Release 9 risks was seen with a link to a more detailed Risk Plan
- The Issues Log was seen to include an entry for a closed issue (Ref. MMGA Issue 0103) with details of analysis, progress review and reason for closure
- The format and contents of Weekly Project Progress Reports are similar to monthly reports and include slides for Release 8.5, 9 and 10 (proactive planning with Client's Project Managers)
- Post Office Account Demand Planning Forum slide pack includes projected staff utilisation
- Joint Programme Board slide pack includes Programme Risks, Programme Issues, Executive Summary, Project Risks & Issues
- Both of the above slide packs are effectively the monthly programme reports which are fed into the Demand Planning Forum and Joint Programme Board. Minutes of this meeting were seen to include a standard agenda, and details of New actions, Previous actions and Closed actions.



Move Forward with Confidence



4.3 Infrastructure Solutions Design and Development (IDBM) – Andy Hemingway, Timothy Salisbury, Dave Ibbett

Assessment Evidence: Microsoft Project_Inf_detailed 130927, Network Management Low Level Design for Release 10 (Ref. DEV/INF/LLD/0045 Version 1.0 dated 15/10/13), SYSMAN Support Tasks for HNG-X High Level Design for Release 10 (Ref. DES/SYM/HLD/0044 Version 2.0 dated 10/9/13), Post Office Account Channel Integration NCR CP1047/CT1321 Network Design (ref. no. 103906-001), IS104762-002-DAB-IS103906-001 Post Office Account Branch New Internet Transit Low Level Design (DEV/INF/LLD/2135 V0.2), ISN006621 DAB Closure Codes, Post Office Account Refresh Change Paperwork V1 spreadsheet

- The Project Plan covering Releases 10, 11 and 12 for the Tech Refresh Programme was seen.
- Within the Café VIK Document Management (Dimension tool) both the SYSMAN Support Tasks for HNG-X High Level Design and the Network Management Low Level Design for Release 10 were seen with the Security Risk Assessment consideration included on the front page and within Section 0.10
- Other documents seen included Post Office Account Channel Integration NCR CP1047/CT1321 Network Design and the Post Office Account Branch New Internet Transit Low Level Design
- The RIO process is used to request resource as subject matter experts to be involved in DAB review.
- DAB Closure Codes includes both Approval Codes and Rejection Codes (such as R009 – Reject comments)
- It is understood that MSC is reviewed by other Fujitsu business units for impact and that all changes are assessed and approved by the Fujitsu sponsor
- It was explained that Managed Service Change (MSC) is used for the Release 10 Infrastructure Change Management and the Post Office Account Refresh Change Paperwork spreadsheet was seen to include a list of MSC references and associated RIO references.
- A closed change example (Ref. 043J0381417-09) was seen to include Description and template fields completed with details/responses and record of how change was requested.

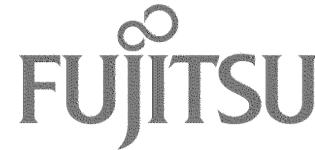
4.4 BMS, Internal audit, Corrective action, Continual improvement, Quality and Security Management Review, Performance Dashboard, Physical and environmental security – Bill Membery, Neneh Lowther

Assessment Evidence: Quality & Compliance Framework Version 5.0 dated 29/7/13, POA Application Design & Build (APT) Process Waiver Request Form, POA Integrated Audit Schedule 2013-14, POA Corrective Action Log, Assessment Database, Quality Management Report dated August 2013, Quality and Security Management Review presentation pack for October 2013, Security Assessment Issue 1.0 dated 9/9/13, Continuous Improvement Tracker, Business Management Performance Dashboard

- The Quality & Compliance Framework (Implementation Approach Document) includes cross-reference to Post Office Limited standards. Within the online area UK&I Process Waivers an entry was seen for Post Office Account Application Design and Build (APT) with start date 1/6/13, next review date 12/1/14 and expiry date 31/5/14. The Process Waiver Request Form was seen to include:
 - Justification Summary
 - Business Justification
 - Attachments
 - Approvals
- The POA Integrated Audit Schedule includes entries for:
 - POA Internal Security Audit April 2013 started on 11/4/13 raised 4 NCRs and 7 Observations
 - Internal Health Checks
 - Programme & Project Management June 2013 identified 8 issues for improvement



Move Forward with Confidence



- The POA Corrective Log contains no outstanding actions and the list of all completed internal audit actions with closure details was seen within the Assessment Database.
- The Continuous Improvement Tracker included 3 remaining improvements identified from the Programme & Project Management internal audit. Also seen was an entry for a closed improvement (Asset Management – phase 1) which included details of Activity Progress and closure details. Another improvement that has been implemented resulted in documents being regularly reviewed.
- The presentation pack for the October 2013 Quality and Security Management (held quarterly) was seen to include both existing and new QMR Action items.
- The Business Management Performance Dashboard was seen to include details on:
 - Quality and Compliance
 - Customer Satisfaction
 - Document Management
 - Management Information Systems
 - Business Risk Management
 - Corporate Social Responsibility
- The following aspects were evidenced during a walking site tour:
 - Security barriers fitted for car park entrances/exit
 - External security lights and CCTV cameras installed
 - Most staff enter the building via a one-pass turnstile requiring their access card to pass through
 - Visitors are directed to the Reception entrance which is manned during office hours and includes barriers requiring staff access cards to be used for entry and exit. Visitors are required to sign in and are issued with visible passes to be worn. The auditor's pass was checked and confirmed as not allowing entry / exit around the office and to / from the building entrance areas.
 - The Security Office manned by external contractor MITIE staff was visited where the external and internal camera systems were confirmed as operational. Contractors are required to complete sign in log for issue of access passes and keys for the purpose of their work visit.
 - An additional building entrance next to the Security Office for the use of Facilities or in case of emergency was seen fitted with pin code access.
 - The main POA office is located on secure floor 4 and contains a further secure area office within. Bins for Confidential Waste Only were seen along with printers/copiers fitted with SAFECOM staff access pass system.

4.5 Implementation & Test Services – Mark Ascot

Assessment Evidence: Horizon Online System Validation and Integration Release 9.0 Test Plan Ref. TST/SOT/HTP/2335 Version 0.1 dated 23/7/13, Minutes of Cycle 4 SV&I Release 9.0 Test Readiness Review dated 4/9/13, Horizon Online System Validation and Integration Release 9.0 Test Report Ref. TST/SOT/REP/2283 Draft Version 0.2 dated 14/10/13

- It was explained that there are two test teams – System Validation and Integration (SV&I) and Live System Team (LST) and a Release Test Plan was seen to include new tests and a section for Regression Testing.
- An example of Test Readiness Review records was seen to include a set of criteria questions with responses provided in NOTES column
- Using the Quality Center tool a subset number of cycles of tests are run as functionality / changes become available for testing. Within Cycle 1 it was seen that groups of test runs for CP0875 for Extended Hours Batch Processing. Test Instance Properties shows details of Test Steps and recorded that Step 3 Failed. This resulted in Defect ID 18814 being raised which subsequently confirmed the fix was accepted.



Move Forward with Confidence



- An example of a Test Report was seen to include Test Cycle Summaries for each cycle with details of test and defect metrics.
- Post-test review is conducted as part of the Service Readiness Review. An example of a Release Authorisation Records was seen to include embedded final LST Test Plan which records all tests performed and completed with status achieved.

4.6 Security documentation and management functions, Security Health Checks, ISMS improvement, Information Security Incident Management – Tom Lilywhite, Kumudu Amaratunga, Chris Cole, Dave Haywood

Assessment Evidence: POA Information Security Policy Ref. SVM/SEC/POL/003 Version 5.3.1 dated June 2013, Post Office HNG- X Account ISMS Manual Ref. SVM/SEC/MAN/003 Version 3.1 dated 13/9/13, SOA Version 9.0 dated 29/11/12, Design Security Template Ref. DES/GEN/TEM/2265 Version 0.1 dated 2/7/13, HNG-X Technical Security Architecture Ref. ARC/SEC/ARC/003 Version 3.0 dated 12/5/12, HNG-X Security Focused Re-Testing Version 7.0 dated October 2013, Security Improvement Plan 2013-14 Version 1.1 spreadsheet, POA Operations Incident Management Procedure Version 5.2 dated 24/10/13, TFS Security Incidents Oct 2012-Sept 2013 spreadsheet

- Within the Dimension Document Management System the following were evidenced
 - POA Information Security Policy – it is understood that a newer and simplified version will be circulated for senior management review and approval
 - Post Office HNG- X Account ISMS Manual explains how within Fujitsu the ISMS controls are applied to the Post Office Account
 - SOA justifies exclusion to A.10.9.3 controls and consideration is being made in also justifying exclusion to A.11.5.6 controls.
- Documents also evidenced were the Design Security Template and the Technical Security Architecture which describes the technical security framework for HNG-X.
- The STREAM Risk Management Tool is used for live/residual risks and to measure risk against Confidentiality, Integrity, Availability and Legal aspects. For each of the 39 entries (none identified as high risk) there is a Risk Treatment Plan link and this was evidenced for entry FJA-A-001.
- Security Health Checks are undertaken and evidence of penetration testing undertaken by the NCC Group in October 2013 was seen to record a number of issues. Two of these issues are outstanding (HNG-X 2-8 and HNG-X 4-3) and the latter is now controlled with an associated Risk Treatment Plan which was evidenced.
- The Security Improvement Plan spreadsheet was seen with 12 entries (5 completed) including 11-2013 Training & Awareness improvement along with dated updates within the Comments column.
- The POA Operations Incident Management Procedure used for security incidents was evidenced. The Triole For Service (TFS) Security Incidents spreadsheet contained entries which were all closed and had cross-references to TFS helpdesk ticket numbers. An example of a Priority 2 incident (A2290792) was seen to relate to Notification of Zero Day Exploits which was raised and closed on 8/02/13 and included resolution actions undertaken.



Move Forward with Confidence



4.7 Applications Solutions Design and Development – Nick Lawman

Assessment Evidence: HNG-X DBM System Design, Code, Build & Component Test Issue 5.0 dated 1/5/13, HBS Recovery Service High Level Design Ref. DES/APP/HLD/2063 Version 1.0 dated 1/2/13, Counter Reports Low Level Design Ref. DEV/APP/LLD/0179 Version 4.0 dated 28/2/13, Code Review Checklist (Generic)- Sign Off Form POA HBS Configuration Ref. DEV/GEN/TEM/003 Version 1.0 dated 12/4/12, HBS Recovery Component Test Plan Ref. DEV/CNT/CTP/2064 Version 1.0 dated 18/3/13, HNG-X Secure Coding Guidelines Ref. DEV/APP/WKI/1979 Version 1.0 dated 2/4/13

- For the 2013 Release 8 it was explained that the standard waterfall development lifecycle was followed as described within the System Design, Code, Build & Component Test document
- Examples of High Level and Low Level design documents were evidenced along with Secure Coding Guidelines which included requirements for PCI DSS.
- An example of a Code Review Checklist (Generic) – Sign Off Form was seen to include tabs for:
 - List of readable code files
 - Review assessment – checklist for consideration of coding standards, safety, security, correctness, completeness, maintainability, traceability, supportability
 - Action list – reviewer's comments with response from developer
 - Instruction – guidelines on how to do code review
 - Resources –cross-reference to many coding standards including Open Web Application Security Project (OWASP) which includes information on injection attacks and insecure cryptographic storage
- An example of a Component Test Plan was seen to include test definition and high level summary result statement.
- Different server environments are used for unit test (development), testing by the Integration Test Team and for the live system (Production).
- Along with MS Visual Source Safe the configuration management of software is also implemented using Dimensions.
- It is understood that a Statement of Work and a Service Agreement are in place for the management of 4th line application support provided by the Fujitsu GDC team located in India.

4.8 Application Implementation and Support – Steve Parker

Assessment Evidence: Peak call references PC022948, PC0226087, Capacity Report Sep 13 spreadsheet, February Capacity Review Minutes

- It was explained that the Peak Incident Management System is used for the 3rd line application support service in dealing with incidents escalated from 1st and 2nd line help desks.
- An example of a Priority A call raised on the day of the audit at 9.46 am was reviewed. A banking transaction system had stopped and with a 1 day SLA target the call had already been assigned to a SSC team member.
- An example of a closed call reported in HNG-X Release 6.5 concerned Postmaster getting an error message. After investigation it was confirmed that the Postmaster was trying to access an unavailable transaction and a confirmation message was sent in response.
- Monthly reports are generated and monthly meetings are held concerning capacity management. A report was seen showing the transaction volume data for different services. Meeting minutes were evidenced of a discussion about VOCALINK and the impending breaches of contracted volumes.



Move Forward with Confidence



4.9 Change Control – Alan Flack

Assessment Evidence: Change references 043J0387875, 043J0387875-03 and associated records

- It was explained that there are two types of change control: Business Change Control (usually generated by customer) and Operational Change Control (includes normal business changes such as fixing broken server).
- All changes involve risk assessment, method statements and approvals and the Managed Service Change (MSC) tool is used to automatically log all activities of users.
- An example of a current (master/parent) change currently in the Stage 4 Build was seen to include details of description, responsibilities and approval. Also evidenced was a link to Filestore for a copy of the release note which is recorded within the Peak Incident Management System and the completed RFC Impact Assessment. This change has been tested by System Validation and Integration (SV&I) and will be progressed through Stage 5 Implement to the final Stage 6 Close.
- An example of one of the associated sub/child changes which had been tested by Live System Test (LST) and closed was also reviewed. Within Filestore the following was evidenced:
 - RFC Impact Assessment for Master RDT MSC for Major R9 Extended Hours and OSR Messaging
 - Deployment Plan
 - Acceptance Post Implementation Review

4.10 Service Desk, Operational Business Change, Service Management, Monitoring and Reporting – Leighton Machin, Sandie Bothick, Mark Jones

Assessment Evidence: TFS reference A3120381, September Service Overview – CSAT slide, Service & Commercial Review – October 2013, USAT monthly spreadsheet, Branch Network Service spreadsheet, Service Desk spreadsheet, KPI Dashboard

- An example of an Operational Business Change (OBC) refurbishment for POL branch was reviewed and a slide for the September Service Review – CSAT and Service & Commercial Review – October 2013 were also evidenced.
- It was explained how agents are set up to access the TFS and other systems with SLTs defined (e.g. to answer phones). Two weeks' induction training is provided for new agents and calls coaching KPIs are set for recorded calls. Trend analysis is undertaken to reduce demand and re-configure the shift pattern to make sure SLTs are met.
- Polling of client and users is recorded within the USAT monthly spreadsheet and a Branch Network Service spreadsheet and Service Desk spreadsheet were also evidenced.
- Through Café VIK the following aspects of the KPI Dashboard were seen:
 - Quality and Compliance
 - Customer Satisfaction
 - MIS
 - Business Risk Management
 - Corporate Social Responsibility



Move Forward with Confidence



4.11 Data Centre Delivery, Planned Preventive Maintenance, Business Continuity Testing – John Hill

Assessment Evidence: IRE11 Access Card Control Sheet spreadsheet, IRE11 Monthly Access Card Report spreadsheet, NI Data Centre Clearances Updated 121001 spreadsheet, Belfast DC PPM 2013 (Working Copy) spreadsheet, Hosting, Networks & Security First Response Guide for IRE11 (Ref. No. ISN003443 Version 4.4 dated 10/6/10), POA Loss of HNG-X Active Data Centre IRE11 Business Continuity Test Plan (baselined 4th May 2013)

- It was explained that 2 data centres in Ireland are used to host POA equipment and that to request site access all necessary visit details need to be provided through the online Data Centre Portal. An access request (Visit ID IRE11-A101171) raised on 30/10/13 for access on 31/10/13 was seen along with cross-reference to an associated TFS 21331 ticket.
- Access to the Technical Halls requires use of a personal access card as well as entry of a PIN code and all rack cabinets are further locked down by key.
- The following access records were evidenced:
 - IRE Access Card Control Sheet spreadsheet showing details of cards allocated to Fujitsu engineers and reason for their access
 - IRE11 Monthly Access Card Report spreadsheet to Tech Hall 1 and Tech Hall 2 showing details of issued card use
 - NI Data Centre Clearances Updated 121001 spreadsheet from the Fujitsu NI Security Administrator
- This year's Planned Preventive Maintenance spreadsheet for the Belfast Data Centre was seen to include entry 043J0393862 Biannual Water Leak Detection Maintenance as well as the Status column being used to confirm completion activities with cross-reference to any relevant PEAK ticket.
- It was explained that whilst there is no specific BCP for the POA a planned campus failover was recently undertaken. At the time of the audit the results and lessons learned from this DR test were awaiting review and filing.

4.12 Finance Management Reporting – Matthew Church

Assessment Evidence: Business Review Monthly POA October V3, Q3 Budget Summary Spreadsheet Prt8

- Responsibility for pulling together robust financial reports was explained with Actuals being checked at month end and Forecasts drafted for future planning.
- A quarterly budget is produced and the Q3 Budget Summary spreadsheet was seen along with an example of a monthly Business Review.



Move Forward with Confidence



5. OBSERVATION

The following Observation was raised during the course of this assessment

5.1 Observation Ref.1

Reference / Sequence	1	Date of Observation	31/10/13
Category	Observation	Standards / Section	ISO 27001 8.2.2
Corporate Process	<i>Input by Fujitsu</i>	Local Process	<i>Input by Fujitsu</i>
Unit	Post Office Account	Country	UK / Ireland
Location	BRA01	Division	BAS
Interviewee	Tom Lilywhite	Interviewee's Role	CISO
Area Contact	Bill Membery	Assessor's Name	Paul Bonnet

Observation

Staff may not have received appropriate awareness training and regular updates in organisational policies and procedures as Corporate security training was last provided about 18 months ago.

Notes

This risk has already been identified within the Post Office Account and it is understood that:

- A number of security awareness activities have been undertaken with the POA team in 2013
- The CISO plans to re-introduce formal security training by Q2 2014