FUJ00232700

Post Office Ltd,
Finsbury Dials,
20 Finsbury Street,
London, EC2Y 9AQ

CONFIDENTIAL – COMMERCIALLY SENSITIVE

Wendy Warham

VP Digital Transformation and Innovation

Fujitsu

22 Baker Street

London

W1U 3BW

20/8/2020

Dear Wendy

Re: Horizon Audit

After your discussions with Jeff Smyth regarding the above I am giving notice that we would like to perform an audit of Horizon in line with clause 25.2 and Schedule D5 of the Horizon contract.

In line with Section 25.2:

1. Fujitsu must provide reasonable access to Records and all reasonable assistance for an audit to confirm FJ's compliance with the Agreement. We are giving Reasonable notice via this letter.
2. This audit will cover the last six years' worth of records.
3. Each party is to bear its own costs.
4. We must agree arrangements relating to the audit with you, but such agreement should not be unreasonably withheld or delayed.
5. More details of the audit are included in the attached Terms of Reference, In summary:
    i. We intend to start the audit from week commencing 7 September 2020.
    ii. The audit team will be led by Tony Jowett as our Interim IT Director supported by other Post Office personnel and a team from our data analysis partner BDO. Names of the key personnel will be provided closer to the time.
    iii. We will need a point of contact and associated team within Fujitsu to facilitate access to data as per the ToR.
    iv. We anticipate the initial phase of the audit will take 3-4 months – subsequent phases are likely and are to be defined
    v. We will provide Fujitsu with a report at the end of each phase setting out:
        a. Areas of non-compliance which FJ must rectify; and
        b. Any recommendations regarding the provision of the Services and potential changes to the Agreement.

FUJ00232700

Fujitsu will have 30 days to review the report and comment on recommendations.

I would be grateful if you could confirm your arrangements regarding this audit, including the name and contact details of the person you nominate to act as a primary point of contact, as soon as possible.

I look forward to hearing from you.

Yours sincerely

Tony Jowett

Interim GLO IT Director

GRO

FOR AND ON BEHALF OF POST OFFICE LIMITED

Enc: As stated

FUJ00232700

Post Office IT Controls - TERMS OF REFERENCE

Background:

The Horizon Issues Judgement Findings (HIJF) identified a series of remediation actions that Post Office should undertake relating to Horizon functionality and associated IT controls. Accordingly, Post Office intends to commission independent audit(s) to validate the efficacy of key process controls and to confirm that all historic Known Error List (KEL) items have been eliminated in HNGA.

It is incumbent upon Post Office to ensure those organisations responsible as "Data Processors" are providing services appropriately, aligned to Post Office principles and goals, business targets, industry or vendor based best practices. Therefore, audit(s) shall address key capabilities as provided by major service towers as defined within the "scope of audit".

Post Office Group IT is measured against an existing 27001, COBIT and NIST control framework(s); however, Post Office recognises that tower suppliers have and may maintain their own respective controls, processes and procedures which may not be in strict alignment to Post Office standards. These audit(s) will seek validation through strict evidence-based assessment and data sampling, assurance of key IT and management controls, policies, and procedures adherence. Where appropriate for controls management the audit(s) will seek confirmation of actively managed remediation plans, risks/issues and dependency tracking aligned to the overall governance frameworks for the tower supplier.

Rationale for Audit:

The key drivers for the audit(s) are a combination of HIJF and a general objective to continuously improve the overall IT control environment. For some, but not all, tower suppliers, recent major incidents have triggered a need for additional control assurance.

Key Risks:

The following Post Office principal risks areas are to be addressed in this review:

- Change Management, including SDLC activity
- Incident Management and Response
- Cyber security
- Privileged Access Management
- Service Monitoring (including capacity planning, end of serviceable life management)
- Technology operations
- Dependence on 3rd parties and contract management
- Information protection

FUJ00232700

Scope of Audit:

The audit will provide a detailed assessment of capability in all listed areas and will carry out focused analysis in service affecting areas.

These capabilities are as follows:

- Overall IT Controls including but not limited to domains covered by COBIT 5, ISAE 3402
- Policy Adherence and Alignment to Post Office standards
- Management Oversight & Accountabilities of the IT controls environment

As key functions too:

- Pre, during and post Change Management
- Pre, during and post Incident Management
- Joiners-Movers-Leavers process management and access controls
- Privileged User Access Management
- Management of Known Error List (KEL) items – historic and current
- Management of Remote System Access (counters and central servers. databases)
- Cyber Assurance

Relevance also applies to:

- Interface to Post Office Service Management
- Interface to Other Tower Service providers

Furthermore: following pre agreed review milestones dependant on the investigation outcomes Post Office CIO reserves the right to extend the audit in key areas where concerns by the external auditors have been raised. These may include but not be limited to:

- Security event monitoring
- Service event monitoring
- Security Platform Admin and Ops
- Data loss prevention
- Information lifecycle management
- Data privacy
- Information classification
- Human resources security
- Identity lifecycle management
- Policies, standards & architecture
- Cloud security
- User access control

Detailed scope and timescales of the audit is to be confirmed by the audit team and audited organisations.

FUJ00232700

Stages and Timeline: (dates TBC, but ASAP)

Field Work pre assessment

Field work

Interim Report 1 High-Level findings

Interim Report 2 findings reassessment

Detailed findings focus areas review

DRAFT Report 1

Final Report (findings relevant to individual suppliers will only be shared with that supplier)

Reporting:

The report will be summarised for the Group CIO, Risk and Compliance Committee and the Board Audit, Risk & Compliance Committee.

Audit Team:

A dedicated team consisting of a combination of POL and external resources to cover the full range of business and technical requirements.