WITN03680200

Witness name: Simon Geoffrey Oldnall

Statement No: WITN03680200

Dated: 30 April 2024

POST OFFICE HORIZON IT INQUIRY

SECOND WITNESS STATEMENT OF SIMON GEOFFREY OLDNALL ON BEHALF OF POST OFFICE LIMITED IN THE POST OFFICE HORIZON IT INQUIRY

INDEX

Section	Sub-section	Paragraph numbers
Introduction		1 - 12
Question 3 of the rule 9 request	3(a)	13 - 31
	3(b) - Introduction	32 - 36
	3(b) 1999-2006	37 - 136
	3(b) 2006-2013	137 - 161
	3(b) 2013-2019	162 - 238
	3(b) Remote access	239 - 364

WITN03680200

	3(c)	365 - 368
	3(d)	369 - 394
Question 4		395 - 500

I, *SIMON GEOFFREY OLDNALL*, of 100 Wood Street, London EC2V 7ER, say as follows:

Introduction

1. I am the Horizon IT Director at Post Office Limited ("**Post Office**"). I have been employed by Post Office since September 2020 in this role. This is my second Witness Statement to the Post Office Horizon IT Inquiry (**"the Inquiry"**).
2. This witness statement has been prepared in response to the 48th request made to Post Office by the Inquiry pursuant to Rule 9 of the Inquiry Rules 2006, dated 10 October 2023 (the **"Rule 9 request"**). I provide with this witness statement a separate note from the Post Office in relation to questions 3(e) and (f) of the Rule 9 request.[1]
3. Consistent with the Rule 9 request, I use "**Fujitsu**" to refer to Fujitsu Services Limited and ICL Pathway Limited, the latter having been acquired by Fujitsu Ltd between 1990 and 1998 and re-branded from April 2002.[2] I use Post Office to refer to the current Post Office organisation and its predecessors.

[1] POL00424367

[2] POL00393860

WITN03680200

4. I have sought to include within this witness statement evidence relating to matters or issues detailed in the Rule 9 request insofar as the relevant facts are within my own knowledge. I have also prepared a glossary of terms referred to in this witness statement.[3]

5. The facts in this witness statement are true, complete and accurate to the best of my knowledge and belief.

6. The Rule 9 request sought evidence relating to some matters and issues that are not within my knowledge. As a result, where my knowledge has been informed by another person or by documents that I have reviewed for the purposes of preparing this statement, I will specifically acknowledge the identity of the individual concerned or the nature of the documents. By way of example, the Inquiry will see at paragraph 33 that I have set out in some detail the approach that I took to preparing my response to questions 3(b)-(d) of the Rule 9 request, due to my lack of any personal knowledge of the matters that are the subject of those questions.

7. I have been assisted in preparing this witness statement by Burges Salmon LLP and Fieldfisher LLP (together **"BSFF"**), who act on behalf of Post Office in the Inquiry (other external advisers also act for Post Office) and external counsel.

8. Where I refer to specific documents in this statement, copies of those documents have (where possible) been produced to the Inquiry.

9. In drafting this statement, and as agreed with the Inquiry in correspondence regarding the approach to the Rule 9 request, I have referred the Inquiry

[3] POL00424366

WITN03680200

(whether in the body of the statement itself or in the footnotes) to a single or small number of examples of documents that explain the processes and procedures that Post Office had in place during the periods that are the subject of the Rule 9 request.

10. In some instances, there are other examples of these types of documents that have been located during the review process for this Rule 9 response. Where Post Office has identified such documents, I have not referred to them all in the statement but I confirm that Post Office has disclosed them to the Inquiry. I make it clear at the outset that Post Office has not conducted searches in order to identify every example of every type of document, e.g. every set of meeting minutes or papers for every forum. As agreed with the Inquiry, such an exercise was beyond the scope of the Rule 9 request.

My role at Post Office

11. I joined Post Office in September 2020, prior to this I was employed for 20 years by a number of consultancy and technology companies, primarily focussed on the delivery of technology enabled change programmes in the UK and overseas. Before then, I spent 10 years in the UK civil service working for the DWP, its predecessors and related agencies.
12. In my role as IT Director for Horizon, I am responsible for:

    a. managing the Post Office Horizon Leadership team and working with third party suppliers involved in the Horizon IT system ("**Horizon**"), which is made up of various sub-teams which focus on different aspects of the Horizon IT System (including Postmaster Experience, Commercial

WITN03680200

Management, Quality Assurance, Horizon Live Services, Remediation and Change as well as Security, Risk & Investigations).

b. designing and implementing changes following the GLO litigation to ensure that Post Office IT takes steps to resolve issues identified in the Horizon Issues Judgement.

c. supporting the Post Office Group Chief Digital Information Officer ("CDIO") and forming part of the Post Office Technology Leadership team.

Question 3(a) - Post Office's position on the nature and extent of the relevant contractual obligations and how they changed over time.

13. In paragraph 2 of the Rule 9 request, "relevant contractual obligation" is defined as meaning any contractual obligation owed by Fujitsu to Post Office Limited (or its predecessors) in relation to:

a. the identification, investigation, recording and reporting of (i) bugs, errors and defects in the Horizon IT system; (ii) other network and system failures or (iii) the impact of such events upon branch accounts ("paragraph 2(a) of the Rule 9 request");

b. the adoption of measures to rectify bugs, errors and defects in the Horizon IT system ("paragraph 2(b) of the Rule 9 request");

c. the use of access rights and privileges by Fujitsu employees to remedy errors in transaction data and branch accounts (paragraph(c) of the Rule 9 request).

14. There have been four overarching contracts between Post Office and Fujitsu, which are as follows:

WITN03680200

a. Preliminary Contractual Agreements: 15 May 1996 – 28 July 1999

b. The “Original Codified Agreement": 28 July 1999 – 31 December 2002

c. The “2002 Agreement": 31 December 2002 – 31 August 2006.

d. The “Current Contract”: 31 August 2006 – present.

15. There is limited corporate memory and documentation in relation to the history of the Post Office and Fujitsu contract. As a result, the detail and information that it has been possible to include within this statement has been compiled through the review of documentation that has been identified for the time periods detailed above and through discussions with individuals who do still have some corporate knowledge regarding the matters that are the subject of the Rule 9 request.

Preliminary Contractual Agreements

16. On 15 May 1996, the Secretary of State for Social Security acting through and on behalf of the Department of Health and Social Services for Northern Ireland ("DSS") entered into an agreement with Post Office for the development and establishment of computer services by Fujitsu. The agreement consisted of three individual contracts which can be summarised as follows:

a. An agreement between the DSS and Fujitsu for services relating to a benefit payment card system ("the DSS Agreement").

b. An agreement between Post Office and Fujitsu for the provision of Post Office infrastructure and other service ("the POCL Agreement").

WITN03680200

c. An agreement between DSS, Post Office, and Fujitsu for the supply of other general services which applied to both DSS and Post Office ("the Authorities Agreement").

17. Following delays to the development and deployment of services under the Preliminary Contractual Agreements, a review of the project was carried out and was led by HM Treasury and involved both the DSS and the Department of Trade and Industry ("DTI"). Thereafter, on 24 May 1999, Post Office and ICL Pathway entered into a Letter Agreement which set out how the relevant aspects of the POCL Agreement and the Authorities Agreement would be codified into a single agreement (not involving the DSS), to reflect a new commercial relationship between Post Office and ICL Pathway. The Codified Agreement was the result of the exercise carried out pursuant to the Letter Agreement.

Original Codified Agreement

18. The Original Codified Agreement was in force from 28 July 1999 to 31 December 2002.

19. The Original Codified Agreement was subsequently amended through 11 different versions which are as follows:

a. Original Codified Agreement Version 1, 28 July 1999: POL00399924.

b. First Supplemental Agreement, 20 August 1999: POL00393858.

c. Second Supplemental Agreement, 24 September 1999: POL00325269.

d. Third Supplemental Agreement 18 January 2000: POL00324066.

e. Version 1.1, 28 July 1999.

WITN03680200

f. Version 1.2, 30 November 1999: POL00393858.

g. Version 1.3, 14 April 2000: POL00028202.

h. Version 1.4, 25 July 2000: POL00393914.

i. Version 2, 12 January 2001: POL00043749.

j. Version 3, 19 September 2001: POL00337516.

k. Version 4, 25 June 2002: POL00394103.

l. Version 5, 30 October 2002: POL00337524.

20. The relevant contractual obligations can, in the main, be found in the Original Codified Agreement. I have therefore endeavoured to identify relevant provisions within the Codified Agreement and the associated schedules that contain those relevant contractual obligations. Where the nature and extent of the relevant contractual obligations changed over time, pursuant to further versions of the Codified Agreement, I have detailed the changes under a sub-heading that specifies the Version or Schedule to the Agreement through which the changes were made.

First version of the Original Codified Agreement

21. I have detailed below the provisions from the first version of the Original Codified Agreement (and the associated Schedules) that set out the nature and extent of the contractual obligations. I have specifically listed any clauses, paragraphs or annexes in which the obligations are contained.

22. I have also set out, where it has been possible to do so, in respect of each contractual provision, the corresponding contractual provision to which it relates as detailed in paragraph 2 of the Rule 9 request.

WITN03680200

23. The provisions of the Original Codified Agreement that, in my assessment, relate to relevant contractual obligations are detailed below. I assess that all the clauses detailed below fall within the scope of the relevant contractual obligations defined within paragraph 2(b) of the Rule 9 request.

    a. **Clause 210 – Further Releases – Sub-clause 210.2: "***Fujitsu may issue further releases of software as necessary to remedy defects in the provision of the POL services for the purpose of maintenance of the POL service infrastructure.*"

    b. **Clause 411 – Acceptance of Core System – Sub-clauses 411.2 to 411.4** (see paragraph 104(b) for acceptance requirements)**:** "*Fujitsu agrees that if, following Core System Release* ("CSR")[4] *Acceptance, any fault arises in connection with the Core System which was not identified as an Acceptance Incident but might reasonably have been expected to be identified as an Acceptance Incident prior to this agreement then Fujitsu shall remedy such fault at their expense. Faults are categorised at Schedule A11*".

    c. **Clause 507 – Risk in Products – Sub-clause 507.3:** "*Fujitsu shall as soon as possible rectify any loss or damage affecting the Core System Products and proceed/complete the installation of the POL service infrastructure and performance in line with this agreement.*"

    d. **Clause 810 – Limitation of Liability – Sub-clause 81.13:** "*If in connection with POL's performance of its responsibilities re in-office data migration, there is a breach of integrity or any viruses enter any system*

[4] The original Horizon system implemented in 1999, which consisted of three major components as detailed in 'ICL Pathway Core System Release Contents Description' (POL00393881): Automated Payments Services, Operational Business Change Services and Electronic Points of Sale Services.

WITN03680200

or disk which is provided by a Fujitsu laptop computer, then POL is not liable to Fujitsu nor will it terminate the agreement as a result of any delay or reduction in service levels if such breach or viruses could not have been avoided or mitigated by Fujitsu."

e. **Schedule A11 – Acceptance Procedure for Core System.** The paragraphs of the Schedule as detailed below all, in my assessment, engage the contractual obligations as defined in paragraph 2(a) of the Rule 9 request**:**

i. **Paragraphs 2.1-2.3:** These paragraphs deal with the criteria that the CSR must meet in order to pass the Acceptance Test. This is the process, defined in an Acceptance Procedure, for determining whether a Service meets the relevant Acceptance Criteria, and is therefore sufficiently effective to be evaluated by the Release Authorisation Board for national rollout. Paragraphs 2.1—2.3 stipulated that the associated thresholds for passing the Acceptance Test may not be met if the threshold of Acceptance Incidents is exceeded. Acceptance Incidents are an unusual or undesirable occurrence, or a request for advice and guidance, which are reported in writing by Post Office to the Contractor (Fujitsu) for analysis. Schedule A11 divides Acceptance Incidents into three categories[5] and stipulates the thresholds for

[5] Schedule A Paragraph 7.1 defines these Acceptance faults as follows:
Category (a) failure to meet an Acceptance Criterion essential to the Deliverable or POCL Service shall be designated a high severity deficiency;
Category (b) failure to meet an Acceptance Criterion which is highly desirable for the Deliverable or POCL Service shall be designated a medium severity deficiency;
Category (c) failure to meet an Acceptance Criterion which is desirable for the Deliverable or POCL Service shall be designated a low severity deficiency.

WITN03680200

failing the Acceptance Test. These are one or more high severity (category (a)) faults or more than 20 category (b) faults generally or more than 10 category (b) faults in respect of any one CSR Acceptance Criteria. If faults were identified, then a CSR Acceptance Test was repeated following corrective work by Fujitsu and Post Office would have the right to test for and raise new faults which may be caused by that corrective work or may only come to light because of the corrective work.

ii. **Paragraphs 3.1-3.2:** These paragraphs provided that if CSR Acceptance was not achieved at the end of the trial review period, Fujitsu would be entitled to a period of 3 months to remedy the defaults at its own expense. Should CSR Acceptance not be successfully achieved at end of the second testing period, then Post Office would have the right to terminate the agreement.

iii. **Paragraphs 7.1-7.2:** These paragraphs outlined that Fujitsu was required to analyse each Acceptance Incident and categorise an incident within the set of principles listed. To summarise, these principles contain descriptions such as '*essential*', '*highly desirable*' or '*desirable*' in relation to the deliverable or Post Office service. Depending on the description applied, each Acceptance Incident would be categorised as either '*low, medium or high severity deficiency*.' Alternatively, it may have been classed as another Acceptance Incident which did not fall under one of the defined acceptance criteria detailed above, but which identified a failure to meet any other obligation under the Codified

WITN03680200

Agreement and represented a substantive equivalent fault. These paragraphs also noted that an analysis of an incident by Fujitsu will not by itself be sufficient by way of resolution. The paragraphs go onto state that resolution will only occur when the deficiency or fault has been corrected by Fujitsu and repeated tests occur thereafter without failure.

iv. **Annex 1 to Annex 11:** These annexes provided detail around the Acceptance Tests that have been referred to above, which were tests to check whether any change or update to the system achieved the targets detailed in the given Acceptance Specification approved by Post Office. These tests were required to take the form of one or more trials and reviews. Trials were referred to as including inspecting, demonstrating, running a real or simulated workload and monitoring a particular system being tested over a trial period to verify the system is working correctly and providing the required service to Post Office. A review was defined as including inspections of a system or specific deliverable and Post Office and Fujitsu meeting to review the results.

f. **Schedule A15 – Requirements,** all of which I assess to engage the relevant contractual obligations as defined in paragraph 2(c) of the Rule 9 request:

i. **Paragraph 1.11 – Requirement 473** This requirement outlined that any remote access or access to system should be restricted

WITN03680200

to users specifically authorised by Post Office. It also stated that it shall be possible to restrict the functionality available at an "*outlet*". An "*outlet*" in this context refers to a Post Office branch. There was also a provision that ensured there should be a secure and reliable mechanism for users to suspend and resume access to the system.

ii. **Paragraph 1.19 – Requirement 481:** This requirement set out that Post Office should provide instructions for transaction support to outlets and details of what to do in emergency situations such as the failure of the Post Office service infrastructure.

iii. **Paragraph 1.58 – Requirement 524:** This requirement outlined that the help desk service should deal with calls relating to the hardware including fault diagnosis, maintenance call out, caretaking advice and configuration management.

iv. **Paragraph 1.60 – Requirement 526:** All reported incidents were required to be resolved in line with Service Levels – which was a quantified and measurable standard defined in a series of Service Level Agreements ("SLAs") that were revised during the term of the Codified Agreement.

v. **Paragraph 1.70 – Requirement 537:** This required Fujitsu to carry out system management to ensure changes and faults could be tracked across service boundaries and any changes made to the Post Office services were made speedily and accurately.

WITN03680200

vi. **Paragraph 1.101 – Requirement 698**: Pursuant to this requirement, Fujitsu was required to set up an organised security infrastructure which encompassed virus control, control of software, reporting incidents and the management of fraud and risk during service operation.

vii. **Paragraph 1.122.6 – Requirement 818**: This requirement provided that the Electronic Point of Sale Service (**"EPOSS"**) needed to include features to check internal consistency, report errors, warn of non-critical errors and prevent critical errors, refuse deletions if there was dependent business data which would lead to inconsistency of data within the Post Office service infrastructure, check data consistency and report exceptions.

viii. **Paragraph 1.124 – Requirement 820**: This requirement dealt with EPOSS functionality which included providing a means of controlling user access to data, processes and functions, maintaining the integrity of the system, ensuring ongoing service consistency and ensuring that following an incident there was no corruption of secured data and that a full recovery was effected as soon as possible in an auditable manner. Furthermore, the requirement stated that EPOSS would ensure that the committal process for a transaction was robust and consistent so that a service interruption did not result in an unrecoverable error. Further, it provided, in the event of any failure of any part of the Post Office service infrastructure, that recovery should be performed with minimum disruption to the user and EPOSS

WITN03680200

would warn the user where there was a possibility that data had been corrupted.

ix. **Paragraph 1.134 – Requirement 830:** Pursuant to this requirement, Fujitsu was required to ensure that all Post Office services were supported by contingency plans including fallback transactions that minimised or negated the impact of a failure in any of the Post Office services based on impact and risk assessments which included a testing strategy.

x. **Paragraph 1.136 – Requirement 832**: Fujitsu was required, pursuant to this requirement, to agree with Post Office, before the roll out of EPOSS, that the capture of data at the outlet was complete, accurate and robust. This was necessary to ensure that in the event of fraud, it should be possible to prove that Post Office services were operating without defect and for appropriate transactions receipts to be automatically generated for customers, a copy retained in the outlet for customers, and a copy retained to allow recovery or problem resolution. Further, pursuant to this requirement, an outlet would be able to maintain an audit trail in the event of any failure of the Post Office service infrastructure.

xi. **Paragraph 1.149 – Requirement 891:** Fujitsu was required, pursuant to this requirement, to report reconciliation results to Post Office, including any discrepancies. Any differences, doubtful items or errors were to be resolved by Fujitsu and reconciliation reports and the identification of doubtful items and

WITN03680200

errors were to be delivered to Post Office by 9am the following day. Fujitsu was to make all reasonable endeavours to resolve any doubtful items and errors promptly.

xii. **Paragraph 1.150 – Requirement 894:** Fujitsu was, pursuant to this requirement, to provide Post Office with details of any Post Office service infrastructure failure or file corruption and information to enable Post Office to monitor and/or manage service levels.

xiii. **Paragraph 1.163 – Requirement 913:** This requirement provided that contingency and/or disaster recovery arrangements and user documentation containing information on what to do during a service failure should be available to all users.

xiv. **Paragraph 1.164 – Requirement 914:** This requirement outlined Fujitsu's obligations to provide a help desk service to Post Office and how Fujitsu will be responsible for providing a problem management system dealing with any failures in the system.

g. **Schedule A16 – Solutions:**

i. **Reference Number 468 (which I assess to engage the obligations contained within paragraph 2(a) of the Rule 9 request):** All faults were to be diagnosed with the aid of expert systems by the Horizon System Helpdesk. This paragraph then went on to set out that a field engineer would visit to assist with any fault.

WITN03680200

ii. **Reference Number 472 (which I assess to engage the obligations contained within paragraph 2(b) of the Rule 9 request):** The system was to ensure data security and integrity was maintained in the event of failures of the Office Platform Service ("**OPS**") which was the IT equipment provided by Fujitsu that allowed for the entire range of business at Post Office outlets to be performed.

iii. **Reference Number 523 (which I also assess to engage the obligations contained in paragraph 2(b) of the Rule 9 request):** Fujitsu was to provide agreed levels of support to resolve problems associated with Fujitsu's operational services.

iv. **Reference Number 524 (which I assess to engage the obligations contained in paragraph 2(a) of the Rule 9 request):** The Horizon System Helpdesk service was required to manage all calls relating to the operation, configuration and end-user support of counter terminal equipment, their operating systems, software, application software and processes. Calls were to be categorised and the Helpdesk would provide problem and fault diagnosis and control any necessary hardware or software maintenance activities.

v. **Reference Number 526 (which I assess to also engage the obligations contained in paragraph 2(a) of the Rule 9 request):** Fujitsu was required to ensure all reported incidents were resolved within agreed service performance levels and in conformance with agreed operational procedures. A

WITN03680200

comprehensive analysis of all incidents, their cause and resolution and the service levels achieved was to be produced for review.

vi. **Reference Number 830 (which I assess to engage the obligations contained in paragraph 2(b) of the Rule 9 request):** This section dealt with contingency planning and outlined that Fujitsu, in co-operation with Post Office, would ensure Post Office services were supported to minimise or negate the impact of failure in any part of the Post Office services including but not limited to basing those plans on impact and risk assessments.

vii. **Reference Number 914 (which I assess to engage the obligations contained in paragraph 2(a) of the Rule 9 request):** The Horizon System Helpdesk would provide assistance and fault management to users and Post Office's clients. It outlined the various categories of service calls and how each different level would prompt a different action. By way of example, the level 3 service was invoked when a call could not fully resolve an issue and required escalation to a higher level of technical support or an engineer to perform a maintenance visit. It also provided detail around the operational services of the Horizon System Helpdesk.

h. **Schedule F05 – EPOS Service Management – Paragraph 6 (which I assess also engaged the obligations contained in paragraph 2(a) of the Rule 9 request):** Fujitsu was required to provide Post Office with

service management reports which included service failures, incidents resolved and outstanding, and the review of ongoing actions such as fault correction.

i. **Schedule G01 – POL Infrastructure Service Definition – Paragraph 6 (which also, in my assessment, engaged the obligations contained in paragraph 2(a) of the Rule 9 request):** This paragraph outlined the functions of the Horizon System Helpdesk Service which included: acting as a central point of information on the working state of the POCL Services; keeping customers notified of any scheduled interruptions to the service; assisting in the negotiations between the client and Post Office where interruptions were scheduled; and keeping Post Office informed[6]. The information on the problem management system was to be updated as the problem progressed, and each update should have been accompanied by the details of when it was implemented, what was changed, who made the change and if it was a solution that was accepted by the customer.

j. **Schedule G07 – POL Infrastructure Service Management – Paragraph 6 and Schedule K05 – LPS Service Management – Paragraph 7 (engaging again, in my assessment, the obligations within paragraph 2(a) of the Rule 9 request):** These paragraphs largely repeat much of the detail in Schedule F05 above, in that they

[6] Schedule G01 Paragraph 6.4.1 states that these include, but are not limited to: a) unique problem serial reference, generated automatically by the problem management system; b) customer contact, address, location and telephone number; c) date and time problem occurred; location and telephone; d) date and time problem was reported to the Horizon System Helpdesk; e) Horizon System Helpdesk contact ; f) description of the problem, including frequency of occurrence; g) serial references of similar faults and previous occurrences; h) Hardware Equipment involved ; serial number etc .;i) Software product and release version; j) assessed impact on customers business; k) priority for solution; l) problem category; m) estimated elapsed time to solve problem; n) any change of referral point; o) date and time of referral.

WITN03680200

outline service reporting, the relevant time scales in which a report needed to be provided and what it needed to include.

k. **Clause 210 – Further releases – Paragraphs 3.3.1 and 4.3.1 (engaging again, in my assessment, the obligations within paragraph 2(a) of the Rule 9 request):** In the event that any of the minimum acceptable service targets were not met, Fujitsu was required to provide Post Office with an analysis of the reason for the failure and both Fujitsu and Post Office were required to then agree a rectification and improvement plan to address the failure.

First Supplemental Agreement

24. The First Supplemental Agreement amended some of the provisions of the Original Codified Agreement. I have detailed the amendments that, in my assessment, are or relate to the relevant contractual obligations referred to in section 2(b) of the Rule 9 request below:

a. **Amendment to paragraph 3.1 of the 1999 Original Codified Agreement:** As CSR Acceptance was not achieved by end of CSR Operational Trial Review Period, Fujitsu was entitled to a period of three months from 16 August 1999 in which to remedy the outstanding defaults at its own expense and to re-submit the Core System Release in its entirety for the second CSR Acceptance Test. However, the agreement stated that the only elements of the Core System Release required to be resubmitted for testing in the Second CSR Acceptance Test were those relating to outstanding faults.

WITN03680200

b. **Amendment relevant to paragraph 7.1(a)-(c) of the Original Codified Agreement:** Paragraph 3.3 of the First Supplemental Agreement addressed the categorisation of new faults that might arise during the testing process. It stated that no faults that had arisen prior to end of CSR Operational Trial Review Period could be raised as a Substantive New Fault unless the nature of fault, in Post Office 's reasonable opinion, had changed or its effect, impact, seriousness or frequency had been greater since the end of CSR Operational Trial Period to the extent that it had, in Post Office's reasonable opinion, a material adverse effect on Post Office's business or operations. However, the provisions of the Original Codified Agreement relating to faults appear to have been made less onerous for the purposes of obtaining CSR Acceptance in the Second CSR Acceptance Test. Although a Substantive New Fault categorised as category (a) would prevent CSR Acceptance (and mean that Post Office had the right to terminate the Agreement), no Substantive New Fault categorised as category (b) would count towards the threshold of 10 category (b) Faults in one area or 20 category (b) faults overall (as detailed in para 2.2(ii) of Schedule A11) - thereby making it less likely that the right to cancel would ultimately end up being triggered. In addition, a failure to agree a timetable to resolve a category (b) Substantive New Fault arising after 3 September 1999 would not prevent CSR Acceptance – despite the provisions of para 2.1(iv) of Schedule A11 of the Original Agreement. Any new category (b) faults arising after 3 September 1999 needed, pursuant to the amendment, to have a timetable for resolution agreed by the parties by 15 November

WITN03680200

1999, in default of which either party could request an expert to specify such a timetable, which was binding on parties. If any substantive new category (b) faults remained by 17 September 1999, Post Office would not withhold its agreement to a timetable for resolution proposed by Fujitsu, if the expert has stated in writing that Fujitsu's rectification plan was likely to resolve the fault by date specified therein and resolution by that date would not, in the expert's opinion, be likely to mean that the fault would not have a material adverse effect on Post Office's business or operations.

Second Supplemental Agreement

25. Two sections of the Original Codified Agreement were the subject of amendment in the Second Supplemental Agreement. These sections, in my assessment, are or relate to the relevant contractual obligations as defined in section 2(a) of the Rule 9 request. They were:

a. **Paragraphs 3.1-3.6:** The paragraphs set out new arrangements and a timetable for the resolution of faults that had failed the initial Acceptance Test but had timetables for resolution (as referred to in Part B of Schedule 1, with each Incident's corresponding rectification Timetable detailed at Schedule 2).[7] Paragraph 3.6 introduced new obligations in relation to errors in transaction records or cash account stream records which were caused by faults with the Horizon system -- and *not* caused by users inputting invalid data in outlets or erroneous reference data

[7] Schedule 2 of the Second Supplemental Agreement details a rectification plan that is 5 pages long which contains reference to various Acceptance Incident Numbers that were created pursuant to that Agreement.

WITN03680200

supplied by Post Office. Specifically, Fujitsu was to issue a Manual Error Report to Post Office.[8] If the number of errors exceeded 20 in any week, Fujitsu was to review the process introduced by the accounting integrity control release with a view to enhancing the process and correcting root causes of errors. Thirty days after the end of each month, Fujitsu was to pay Post Office for its costs in dealing with the Manual Error Reports in relation to erroneous reference data provided by Post Office and to co-operate with Post Office to investigate and resolve such discrepancies.

b. **Paragraph 7.1** introduced an Integrity Checking Process for Post Office's Transaction Information Processing System through which Post Office would carry out a check of cash account discrepancies by comparing data it received across the TIP Interface with electronic cash account data it received from Fujitsu. This new paragraph imposed a charge of £229 payable to Post Office by Fujitsu for each discrepancy reported to Fujitsu.

Third Supplemental Agreement

26. Paragraphs 5.2 and 5.3 of the Third Supplemental Agreement contained provisions that, in my assessment, are or relate to the relevant contractual obligations as set out in paragraph 2(b) of the Rule 9 request:

a. **Paragraph 5.2** imposed a new contractual obligation on Fujitsu in relation to incident types that were defined in Schedule 4. This obligation

[8] The process of issuing Manual Error Reports concerned what are described as "*reconciliation principles*" and branch accounts were one of many streams of financial information that were processed through the Horizon system and needed to be reconciled. As a result, it could be any aspect of that financial information, including errors with branch accounts, that could be the subject of a Manual Error Report.

WITN03680200

required Fujitsu to develop, test, deploy and provide Post Office..with reporting in relation to cash account discrepancies.[9] Fujitsu was also required to develop, alongside Post Office, tools, processes and procedures to address reference data issues in relation to certain listed incidents under Schedule 4.

b. **Paragraph 5.3** imposed a new obligation on Fujitsu to, at Post Office's request, have an expert explain the root causes of Cash Account Discrepancies that had not been detected by the Accounting Integrity Control Release and set out measures that should be introduced to prevent these in future.

c. **Schedule G01 – POCL Infrastructure Service Definition – Paragraph 2.2** established agreed improvements to the helpdesk and a timetable for implementation of these improvements as set out in Schedule 1. One of these improvements was a new Helpdesk Forum which was to have a representative from Post Office.

27. In preparing this statement in response to the Rule 9 request, I have also reviewed the subsequent versions of the Original Codified Agreement but in my view these subsequent versions do not contain any further provisions that are new relevant contractual obligations or amend existing relevant contractual obligations.

The 2002 Agreement

[9] The Codified Agreement defines "Cash Account Discrepancies" as differences which arise when the cash account composed by Post Office from individual transaction data sent across the Transaction Information Processing ("TIP") interface is compared with the electronic cash account retrieved from Fujitsu.

WITN03680200

28. On 31 December 2002, the Original Codified Agreement was replaced with the 2002 Agreement between Post Office and Fujitsu. There were a total of 7 versions of the 2002 Agreement which are detailed below:

    a. Original 2002 Agreement, 31 December 2002 (POL00325101)

    b. Version 2, 6 August 2002 (POL00324108)

    c. Version 3, 5 November 2003 (POL00324122)

    d. Version 4, 26 August 2004 (POL00324132)

    e. Version 5, 5 July 2005 (POL00324165)

    f. Version 6, 30 November 2005 (POL00324169)

    g. Version 7, 15 August 2006 (POL00324187).

29. It is my assessment that only the following clauses from that version are, or relate to the relevant contractual obligations:

    a. **Clause 6.2:** This Clause provided that Fujitsu could issue further releases of software from time to time as necessary to remedy defects in the provision of the services or for the purpose of maintenance of the Horizon Service Infrastructure or the applications. It is my assessment that this clause engages the contractual obligations contained in paragraph 2(b) of the Rule 9 request.

    b. **Clause 9.3.1:** All components of the Horizon Service Infrastructure were required to operate in accordance with their respective specifications, except that, for the avoidance of doubt, it was agreed that Post Office

WITN03680200

should have no remedy for a breach of this undertaking in relation to errors or interruptions to services which were caused by a failure of a Service Level Target (**"SLT"**) or an Additional Remedy Level ("**ARL**[10].") It is my understanding that what this meant in practice was that Post Office would not be able to allege a contractual breach by Fujitsu (or pursue Fujitsu for associated remedies for any such breach) but could pursue it for SLT or ARL remedies. It is my assessment that this clause engages the contractual obligations contained in paragraph 2(a) of the Rule 9 request.

c. **Clause 17.1:**

i. **Clause 17.1.2:** Fujitsu was required to preserve the integrity[11] of the Post Office's data once Fujitsu has received it, and Fujitsu was required to prevent any corruption or loss of that data. **"POL Data"** is defined in the Interpretations section as any data that Fujitsu was granted access to under the Codified Agreement; which was generated by the Horizon system; or which Fujitsu generated while performing its obligations under the Codified

[10] Schedule 15 to the 2002 Baseline Version defined "Service levels and Remedies". The Schedule defined up to three thresholds in respect of each Service Level as follows:
1.1.1.The level of Service ("Service Level Target" or "SLT") required from Fujitsu Services by Post Office. Not all SLT failures give rise to payment of liquidated damages.
1.1.2 The level of Service which, if not achieved by Fujitsu Services, shall give rise to payment of liquidated damages by Fujitsu Services (the "Liquidated Damage Threshold" or "LDT"). Payment of liquidated damages notwithstanding, a failure of any LDT shall not (on its own) constitute a Default.
1.1.3 The level of Service below the SLT and (if applicable) the LDT which, if not achieved by Fujitsu Services, shall give rise to payment by Fujitsu Services of Post Office's Additional Costs or liquidated damages as described (where relevant) in this Schedule (the "Additional Remedy Level" or "ARL".)
[11] In this context, I believe it would have meant that there was a requirement that Fujitsu ensured that the data was not amended or changed.

WITN03680200

Agreement. Therefore, this included, but was not limited to, the financial data generated by SPMs using the Horizon System.[12]

ii. **Clause 17.1.3:** In the event that POL Data was altered, corrupted or lost in the course of performing the services, Post Office had the option, in addition to any other remedies, to:

a) **Clause 17.1.3.1**: require Fujitsu at its own expense to restore or procure the restoration of the POL data; or

b) **Clause 17.1.3.2**: itself restore or procure restoration of the POL data, and be repaid by Fujitsu any reasonable expenses so incurred.

d. **Schedule 15 – Service levels and remedies.** The paragraphs of this Schedule which I refer to below all, in my assessment, contain contractual obligations of the kind defined in paragraph 2(a) of the Rule 9 request:

i. **Paragraph 2.4** provided that all levels of service should be monitored on a weekly and monthly basis and any failure to meet a service level assessed over that month should be reported to Post Office by means of a monthly Service Review Book detailing all Service Levels and the actual levels of service achieved.

ii. **Annex 2 – Data delivery service levels:**

[12] These include:
"Application Interface Specification Reference Data to Pathway for CSR+" (BP/IFS/010)
"ICL Pathway/Post Office Interface Agreement for Operational Business Change - Product" (CS/PRD/058)
"ICL Pathway/Post Office Interface Agreement for Operational Business Change - Branch" (CS/IFS/003)
"Debit Card MoP Functional Specification" (EF/SER/001)

WITN03680200

Paragraph 1.4: This paragraph and sub-paragraphs detailed Fujitsu's obligations to arrange and undertake a visit to a branch to recover transaction records and to assess whether there had been a failure of service levels. Where Fujitsu had been unable to arrange a visit with a branch for reasons of delay on part of the branch, then the period of delay would, pursuant to this paragraph of the Annex, be disregarded and would not be held against Fujitsu.

iii. **Paragraph 3.3.3:** If any of the Service Level Targets in this paragraph were not met, Fujitsu was to provide Post Office with an analysis of the reason for the failure. Fujitsu and Post Office then were to agree a reasonable rectification and improvement plan to address the failure.

iv. **Annex 3 Banking Services – Paragraph 2.2.1:** Fujitsu was required to record and calculatie the number of Core Network Banking (**"NB"**) Service System Faults which caused the NB system not to be available in any one or more Branches. The NB system is the application which supported banking transactions in Post Office branches, which the Interpretations Schedule states is defined in the CCD 'NBS Definition'[13]

v. **Annex 4 Miscellaneous Services – Paragraph 2:** This paragraph provided that the delay between the occurrence of a

[13] POL00394114

WITN03680200

data error and the issue of a manual error report should not exceed five working days.

e. **Schedule 24 – Banking Implementation. The paragraphs of this Schedule all, in my assessment, engage contractual obligations of the kind defined in paragraph 2(a) and (b) of the Rule 9 request:**

i. **Paragraph 5.3.1.2:** Fujitsu was to provide Help Desk support to resolve technical faults in Horizon Service Infrastructure.

ii. **Paragraph 5.8.2:** Fujitsu was to notify Post Office in writing as soon as reasonably practicable after Fujitsu became aware of any PP Dependency Failure or any matter which would result in such failure. PP dependency related to the provision of PayPal and PIN pad services in Post Office branches.

iii. **Paragraph 6.3**: The 2002 Agreement's provisions concerning the Acceptance of the Network Banking Service were similar to the 1999 Agreement's provisions concerning CSR Acceptance (see paragraph 104(b) for section on acceptance). If Fujitsu failed to Achieve NBS Deployment by the NBS Release Complete Date, this would represent a Default. Fujitsu would have to agree a reasonable time in which to rectify the Default with Post Office. If they failed to meet this revised deadline, the Default would give Post Office the option to terminate the Agreement under Paragraph 8.6.4. As was the Case with CSR Acceptance, Network Banking Acceptance Incidents were categorised according to their severity – and thresholds for each

WITN03680200

level of severity were established. If these thresholds were exceeded, then the Network Banking Service would not meet the criteria for Acceptance. Specifically, these thresholds were:

a. No outstanding High Severity NBS Acceptance Incidents at the Release date;
b. Five or less outstanding Medium Severity Incidents at the NBS Acceptance Date (which required an agreed rectification plan);
c. There was no threshold for the number of Low Severity Incidents – although these should have had a target date to be resolved.

iv. **Paragraph 6.4**: This paragraph deals with the raising of NBS Acceptance Incidents. It addressed how Fujitsu was to raise these if a trial failed, a document subject to a NBS review failed to meet the criteria or where any other trial or pilot did not meet the criteria. It also included a table of severity classifications for each incident and measures such as repeat testing, rectification plans.

The Current Contract

30. The initial version of the Current Contract was dated 31 August 2006. It consists of the versions as set out below:

a. Version 1, 31 August 2006 (POL00324232):
b. Version 2, 24 January 2007 (POL00324248):

WITN03680200

c. Version 3, 6 July 2007 (POL00324286):

d. Version 4, 14 April 2008 (POL00324311):

e. Version 5, 23 February 2009 (POL00324320):

f. Version 6, 7 July 2009 (POL00324356):

g. Version 7, 10 May 2010 (POL00324386):

h. Version 8, 21 February 2012 (POL00324419):

i. Version 9, 13 January 2014 (POL00324460):

j. Version 10, 10 September 2015 (POL00324548):

k. Version 11, 31 March 2016 (POL00324703):

l. Version 12, 3 July 2016 (POL00324743):

m. Version 13 (POL00324964):

n. Version 14, 20 December 2021 (POL00325303).

31. I have reviewed Version 1 of the Current Contract and assess that the clauses detailed below engaged the relevant contractual obligations. It is my understanding that there have not been any revisions of these provisions since.[14]

a. **Clause 12.2:** This clause provided for further releases of software by Fujitsu from time to time as necessary to remedy defects in the provision

[14] As was the case with the Original Agreement, the Current Contract can only be amended in accordance with the Change Control Procedure as set out in Schedule A3.

WITN03680200

of the services or for the purpose of maintenance of the infrastructure, the Horizon Applications and the business capabilities and support facilities. It is my assessment that this Clause engages the contractual obligations as defined in paragraph 2(b) of the Rule 9 request.

b. **Clause 15.1.9:** All components of the infrastructure were required to operate in accordance with their respective specifications, except that, for the avoidance of doubt, it was agreed that Post Office should have no remedy for a breach of this undertaking in relation to errors or interruptions to services which caused a failure of a SLT or an ARL.

c. **Clause 33.1 (which, I assess, engages contractual obligations as defined in paragraph 2(a) of the Rule 9 request):**

    i. **Clause 33.1.2:** Fujitsu was required to preserve the integrity of the POL data once Fujitsu has received such data, and to prevent any corruption or loss of that data. Fujitsu was not to be liable for any loss or corruption of POL data nor for any failure to perform the services if it could prove that such loss or corruption or failure to perform the services was caused by POL data which was lost or corrupted before Fujitsu received it, and that Fujitsu had complied with the validation rules.

    ii. **Clause 33.1.3:** In the event POL data was altered, corrupted or lost in the course of performing the Services, Post Office had the following options, in addition to any other remedies: (a) Post Office could require Fujitsu at its own expense to restore or procure the restoration of the POL data; or (b) Post Office could,

WITN03680200

itself, restore or procure restoration of the POL data, and, in that instance, should be repaid by Fujitsu any reasonable expenses so incurred.

d. **Clause 43.19 (which, I assess, contains contractual obligations as defined in paragraph 2(a) of the Rule 9 request):** Fujitsu was required to provide to Post Office copies of or access to all relevant records produced by Fujitsu in the course of performing the HNG-X Services (records were to include, where produced by Fujitsu, operational change proposals, help desk records, release notes, change logs, firewall logs, event records, error logs and audit records) that Post Office assessed were applicable in respect of such failure or delay.[15]

e. **Schedule B3.1 – HNG-X Services (which, I assess, contains contractual obligations as defined in paragraph 2(a) of the Rule 9 request):** This schedule set out a table (Table A: Operational Services) which included an obligation for Fujitsu to provide;

   i. A Third Line Software Support (service number 9 in Table A) service for the diagnosis of new software incidents occurring in Branches;

[15] Both of these Clauses introduce caveats to Fujitsu's liability to Post Office for failing or delaying the performance of their Service obligations:
43.18.1 states there shall be no liability where there is a failure or fault in the communications links to CAPO or LINK – which were external Banks that Post Office provided banking services to. CAPO supported Post Office account cards, and LINK provided the network of cash machines.
43.18.2 states there shall be no liability where the failure or delay is due to unauthorised access, hacking or fraud through the CAPO or LINK systems.

WITN03680200

ii. A Reconciliation Service (number 12 of Table A) for incident management procedures required to investigate, report and resolve reconciliation and business incidents;

iii. A data centre and an Application Support Service line (number 14 of Table A) for software and system errors which could not be resolved by the third line software support service; and

iv. A CMT service (number 15 of Table A) which was to provide a value add function above the standard incident and problem management.

f. **Schedule B3.4 – Branch Infrastructure – Paragraph 3.4.4 (which, I assess, contains contractual obligations as defined in paragraph 2(b) of the Rule 9 request):** As an alternative to replacing a type of equipment that had suffered catastrophic failure, Post Office could request for Fujitsu to cease to provide or to modify services which were affected by that catastrophic failure.

g. **Schedule B4.2 – Existing Applications – Paragraph 8 (which, I assess, contains contractual obligations as defined in paragraph 2(b) of the Rule 9 request):** EPOSS, Automated Payment System ("**APS**") and the Logistics Feed System ("LFS"), but not NBS (which had a process of recovery of incomplete transactions in the event of a counter failure) were to have fallback transactions that minimised or negated the impact of failure in any of the applicable services which used those Horizon Applications (paragraph 2(b) of the Rule 9 request).

WITN03680200

h. **Schedule B4.4 – Existing Service levels (which, I assess, contains contractual obligations as defined in paragraph 2(a) of the Rule 9 request):**

i. Paragraph 2.2.5(a): In the event that an incident or a major failure of the Production SAP System caused the Production SAP System (situated in the live data centre[16]) to be unavailable, Fujitsu was to notify Post Office of such incident or failure as soon as reasonably practicable. Post Office's advanced distribution system which is installed in all branches. If the notification was not in written form, Fujitsu was required to confirm in writing in accordance with incident management.[17]

ii. **Paragraph 2.3:** All levels of service were to be monitored on a weekly and monthly basis and any failure to meet a Service Level assessed over that month was to be reported to Post Office by means of the Service Review Book produced on a monthly basis detailing all Service Levels and the actual levels of service achieved in that month.

iii. **Paragraph 4 and 5:** The Service Levels that Fujitsu were required to meet could be adjusted if a volumetric threshold was exceeded, for example if more than 13,000 calls were made to the Service Desk in each calendar month. These thresholds were

[16] The Interpretations section of the Agreement states that data centres are linked to Post Office infrastructure. Later in contract, it is stated that a Live Data Centre should be linked to support business capabilities and support facilities – which the Production SAP System was among. There was to be a corresponding Disaster Recovery Data Centre which ensured business continuity in these circumstances. The relationship between the two is defined in 'Data Centre Operations Service: Service Description' SVM/SDM/SD/0003.

[17] The normal practice for incident management was detailed in "Major Incident Process" (SVM/SDM/PRO/0001).

detailed in Annex 5 of Schedule B4.4. The remainder of Paragraph 4 stipulated the ways in which the Service Level was adjusted based on the extent to which the threshold was exceeded. Paragraph 5 then clarified that the volumes that would exceed the threshold for specific services – for example EPOSS or NBS – would be determined by the Contract Controlled document (**"CCD"**) 'Horizon Capacity Management and Business Volumes' (PA/PER/033).

iv. **Paragraph 7.1:** In the event that an ARL specified in Schedule B4.4 failed, Fujitsu and Post Office were to agree a method of rectification and timetable for the resolution of the cause of that failure (a "**Rectification Plan"**).

v. **Annex 2 – Data Delivery Service Levels – Paragraph 1.3:** This paragraph and the subparagraphs that follow dealt with when Fujitsu was obliged to arrange and undertake a visit to a branch to recover transaction records and assessing whether there has been a failure of service levels. In summary, where Fujitsu had been unable to arrange a visit to a branch for reasons of delay on part of the branch, then the period of delay was to be disregarded and would not be held against Fujitsu pursuant to the terms of the Contract.

vi. **Annex 3 – Banking Services:** This Annex identified the way that banking facility performance was to be measured, the corresponding SLTs and ARLs and the calculations of the amounts payable if Fujitsu failed to meet the obligation. Part A

WITN03680200

related to NBS. Fujitsu was to record and calculate the number of Core NB System Faults which caused the NBS not to be available in any one or more Branches. They were also required to provide a weekly MIS Bank Analysis Report. Part B addressed debit card SLTs and ARLs. It stated that Fujitsu was obliged to provide Payment Files in accordance with the CCD 'Debit Card MoP Functional Description' (EF/SER/001). Part B also described the method of calculating any damages that arose from a failure to meet this obligation.

vii. **Annex 4 – Miscellaneous Services**: This Annex detailed the Service Levels and associated damages thresholds for services which did not fall into the Annex 2 or Annex 3 categories. These included TESQA[18] and POL FS[19]. The obligations that related to the specific features of each service were detailed. The required availability of each service, the timeframes within which queries should be responded to and the location and time that data generated by the services should all be uploaded.

---

[18] This is defined in the Interpretations Schedule as "*the software tool made available by Fujitsu Services to Post Office which enables TESQA Users to access the Transaction Enquiry Service*", which "*provides Users with 180 days of (read-only) historical Transaction details, and includes the production of the Reconciliation and Settlement Reports and despatch of REC Files to CAPO and Alliance & Leicester.*"

[19] The services provided by Fujitsu, which are detailed in:
Schedule B3.1;
"Service description for the SAP Hosting Service" (CS/SER/022);
Annex C to the CCD entitled "Data Centre Operations Service: Service Description" (SVM/SDM/SD/0003).

WITN03680200

i. Schedule B6.3 – Acceptance (which, I assess, contains contractual obligations as defined in paragraph 2(a) of the Rule 9 request (see paragraph 104(b) for the section on acceptance):

   i. **Paragraph 2.4.2:** A Requirement for each aspect of the new HNG-X system was for it to be allocated its own HNG-X Acceptance Method. The objectives in allocating HNG-X Acceptance Method(s) (as defined in Annex C to the Schedule – see below) to HNG-X Requirements were to progress toward overall HNG-X Final Acceptance as efficiently as possible - but to simultaneously identify and resolve defects in the HNG-X Acceptance Process as early as possible in order to reduce overall development costs and risks.

   ii. **Paragraph 2.7 – 2.10:** These paragraphs dealt with acceptance incidents (where acceptance criterion has not been met) and how fault reports were to be grouped for management and reporting purposes.

   iii. **Paragraphs 4.5 – 4.6:** These paragraphs and sub-paragraphs outlined how progression of acceptance should occur once various conditions had been satisfied, such as there being no outstanding high severity acceptance incidents, or the number of medium severity incidents being five or fewer and an agreed workaround existed. There was also a workaround in the same way for low severity incidents.

   iv. **Paragraphs 6.1 – 6.4:** These paragraphs and sub-paragraphs set out how incidents were to be managed, analysed and

WITN03680200

rectified. Fujitsu was to report incidents to Post Office who would then jointly analyse and classify severity. Tests might then be repeated and Fujitsu would then prepare a rectification plan.

v. **Annex A** This annex is an HNG-X Acceptance Incident Severity Matrix which categorised each incident as '*High, Medium, Low, Non-Incident*'.

vi. **Annex C:** This annex set out the HNG-X Acceptance Methods. It provided a description to each type of method in respect to acceptance criteria, for example solution tests that were owned and managed by Fujitsu with collaboration from Post Office for the purpose of verifying that Fujitsu's solution for the HNG-X System satisfied the relevant acceptance criteria.

vii. It is important to note that Post Office's remedies were diminished in the HNG-X Acceptance process in comparison with the CSR Acceptance process in the 1999 Agreement and the Network Banking Acceptance process in the 2002 Agreement. There is no clause that gave Post Office a right to terminate the Agreement in respect of an Acceptance Failure that meant that Fujitsu did not meet the Acceptance date – although clauses were in place that prescribed how many Acceptance Incidents would represent a failure to pass through the given Acceptance gateway. Further, Clause 2.9 Clarified that an HNG-X Acceptance Dispute was not a Dispute in the wider context of the Agreement.

WITN03680200

3(b) What, if any, internal or external measures were put in place to monitor Fujitsu's compliance with the relevant contractual obligations

Introduction

32. The period that is the subject of question 3 of the Rule 9 request is 1 January 2000 to 16 December 2019 ("the relevant period"). As I have explained above in paragraphs 11-12, I began my role as IT Director for Horizon within Post Office in September 2020. I therefore do not have any direct personal knowledge or experience of the matters that are the subject of question 3(b)-(d). There is also limited corporate knowledge and associated documentary material within Post Office of the matters that are the subject of those questions.
33. As a result, the approach that I have taken to preparing the response to questions 3(b)-(d) has been as follows:

    a. Post Office's external lawyers, BSFF, have conducted a review of more than 330,000 documents that are responsive to search terms that have been created in response to the Rule 9 request in an effort to identify documents that may assist me in responding to questions 3(b)-(d).
    b. Following that review, BSFF have, in conjunction with external counsel, analysed those documents and prepared a draft statement.
    c. That draft statement and the underlying documents have been provided to me to consider with any associated knowledge gaps being highlighted for Post Office to consider further internally.
    d. I have reviewed the statement and made further enquiries within the Post Office business as needed to satisfy myself to the best of my ability as

WITN03680200

to what the position was within Post Office within the relevant period in relation to the matters that are the subject of questions 3(b)-(d).

e. Where I have satisfied myself as to what the position was, I have set that out in this statement. Where I had further questions, I have asked those, and further investigations have been undertaken internally and externally to answer them. However, where, despite the work detailed above, I have not been able to achieve clarity in relation to matters that are the subject of questions 3(b)-(d), I have made that clear in the statement, so that the Inquiry is aware of the limits of my (and the wider Post Office corporate) knowledge and understanding of those matters.

Summary

34. The ways in which Fujitsu's compliance was monitored by Post Office varied and evolved over time in line with system change, the nature of the services being provided, and the changing nature of Post Office as an organisation. From the outset of the Horizon system, it is therefore my understanding that monitoring did not take place in isolation, but as part of an iterative operational and contractual relationship.

35. It is my understanding that the monitoring of Fujitsu's compliance with the relevant contractual obligations during the relevant period as defined in the Rule 9 request fell within distinct phases of time. I have therefore described the measures that were put in place to monitor the relevant contractual obligations as defined in section 2(a) and(b) of the Rule 9 request for each of those time periods.

WITN03680200

36. I have dealt with the measures that were put in place (whether internally or externally) to monitor the use of access rights and privileges by Fujitsu employees to remedy errors in transaction data and branch accounts (section 2(c)) as a distinct section, as these do not sit as clearly within the date ranges described above because of the complexities associated with Post Office's understanding of those contractual obligations.

INTERNAL OR EXTERNAL MEASURES THAT WERE PUT IN PLACE TO MONITOR FUJITSU'S COMPLIANCE WITH THE RELEVANT CONTRACTUAL OBLIGATIONS AS DEFINED IN SECTIONS 2(A) AND (B) OF THE RULE 9 REQUEST

1999 – 2006

(a) The identification, investigation, recording and reporting of (i) bugs errors and defects within the Horizon IT system; (ii) other network and system failures or (iii) the impact of such events on branch accounts.

37. In describing the internal or external measures that were put in place to monitor Fujitsu's compliance with the relevant contractual obligations below, the Inquiry will note that I have not referred specifically to the measures that were used to identify, investigate, record and report on the impact of events on branch accounts. The reason for this is because the measures that were used by Post Office to identify, investigate, record and report on bugs, errors and defects (**"BEDs"**) and network and system failures (**"NSFs"**) would extend to the impact of those events on branch accounts. There were not separate policies or procedures in place in respect of the monitoring of the impact of events on branch accounts.

WITN03680200

38. It is my understanding that the internal measures that were put in place to monitor Fujitsu's compliance with the matters defined in question 3(b) of the Rule 9 request (in so far as sections 2(a) and (b) of the Rule 9 request are concerned) can be summarised in so far as the 1999-2006 period is concerned as follows:

    a. Governance and Contract Management (paragraphs 39-58)

    b. Service Reviews (paragraphs 59-102)

    c. Testing and Acceptance Requirements (paragraphs 103-115)

    d. Rolling reporting obligations that were placed on Fujitsu.

Governance and Contract Management

39. The relevant contractual provisions dealing with governance and contract management during this period were contained within Schedule A04[20] to the Original Codified Agreement, which provided for 'Contract Management' and Schedule 4 of the 2002 Agreement, which provided for 'Governance'.

40. Pursuant to the Original Codified Agreement Schedule, Post Office and Fujitsu were required to establish the following boards/groups to facilitate that process:

    a. **Change Control Board**

    b. **Contract Administration Board**

    c. **Service Review Board** (see paragraph 59 for Service Review section)

    d. **Contract Steering Group**

    e. **New Business Board**

[20] POL00399922

WITN03680200

f. Release Authorisation Board[21]

41. It is my understanding that both the **Contract Administration Board** and the '**Service Review Board**'[22], which were jointly attended by Post Office and Fujitsu, played a role in Post Office's monitoring of Fujitsu's compliance with the relevant contractual obligations.[23] I understand that the purpose of the **Contract Administration Board** was to review and agree changes to the contract, provide advice regarding Change Control Notices (**"CCNs"**) the drafting of and consideration of Change Requests (**"CRs"**). The purpose of the **Service Review Board** was to review performance against contracted service levels and to agree remedies payable arising from any failures to meet service levels - which I will address in more detail in the Service Review section will set out in further detail below (see paragraph 59).

42. By January 2000, Keith Baines, who in 1999 held the role of 'Head of Commercial' for Post Office Counters Limited ("**POCL**"), drafted a discussion paper that reviewed the structure of joint POCL and Fujitsu meetings, noting that there had been *"some apparent weaknesses in previous arrangements"*. By way of example, one of the weaknesses that was identified was that there had been "*many instances of issues being raised at more than one meeting,*

---

[21] POL00399922

[22] Attendees at the Service Review Board were to be the POCL Head of Service Management and others at their description, and Contractor attendees were to be the Customer Service director, and others at their discretion.

[23] The stated purpose of the Service Review Board was "*to review performance against contracted service levels/to agree remedies payable arising from any failures to meet service levels/to monitor and review operations business change processes*." The stated purpose of the Contract Administration Board was "*to review and agree changes to the contract to implement signed CCNs/To discuss and resolve questions of the interpretation of the contract/To agree mechanisms to enable new provisions to be drafted and agreed under CCN/To provide expert advice on drafting of CCNs/ Contract version control/Maintaining lists of current CCDs and CRDs/Maintaining lists of agreement to agree their status*." It was also separately stated that one of the purposes of the Contract Administration Board was "*to discuss and resolve questions of interpretation of the contract*".

WITN03680200

and lack of clarity in the process for escalation and resolution of difficult issues". It is my understanding that this was noted as being the result of overlapping terms of reference.[24]

43. In his review, Mr Baines proposed that the following committee structure of joint Post Office and Fujitsu Boards, meetings and working groups was set up to improve the ongoing arrangements between POCL and Fujitsu pursuant to the Original Codified Agreement:

    a. **Joint Management Board**

    b. **New Requirements Board**

    c. **Joint Change Control Board**

    d. **Joint Contract Admin and Commercial Board**

    e. **Joint National Rollout Board**

    f. **Joint CSR+ Programme Board**

    g. **Joint Programme Boards for future Releases**

    h. **Service Review Board (headed by the Head of Business Service Management)**

    i. **RollOut Working Group**

    j. **Functional Meetings**

    k. **Operational Service Working Groups**[25]

44. Annex A of the discussion paper appears to have proposed a replacement for the scheme at Schedule A04 of the Original Codified Agreement.[26] It is my understanding that his proposals were then put to Fujitsu Finance and

[24] POL00393888
[25] POL00393888, p.4
[26] POL00393888, p.4-8

WITN03680200

Commercial Director, Tony Oppenheim for consideration[27] and that, thereafter, some of the proposals were adopted (through, by way of example, some of the work of the National Roll Out Board), and that in other respects the arrangements set out in the 1999 Codified Agreement were maintained without amendment.

45. In carrying out a review of documents for the purposes of preparing this statement, I have had sight of correspondence which suggests that the primary responsibility within POCL for the operation of the contract with Fujitsu appears to have sat, up until 2006, with Keith Baines. It is my understanding that any perceived non-compliance with the relevant contractual obligations (for example, data loss by Fujitsu) would be raised on Post Office's behalf in ongoing correspondence between Mr Baines and his Fujitsu counterparts and at meetings of the **Contract Administration Board**. [28][29]

46. It is my understanding that any remedies or changes to the service resulting from correspondence between Post Office and Fujitsu or discussions at **Contract Administration Board** meetings would be expressed and formalised through correspondence. [30]

---

[27] POL00393890

[28] See, e.g., POL00401664, letter dated 27 June 2001; POL00401663, letter dated 10 August 2001.

[29] I have reviewed correspondence that refers to concerns having been raised by Keith Baines at a Contract Administration Board meeting regarding an apparent data loss by Fujitsu for a period of 7 days in August 2000. Reference was made to this having been discussed at a meeting of respective audit and security teams on 20 June 2001. During the course of the meeting, Post Officeexpressed concern as to how long "*an issue of this magnitude*" was taking to resolve and stated that Fujitsu should have in place a process which alerts Post Office to any failure of their obligation to maintain a full audit trail, irrespective of whether Post Office has requested data during the course of a particular period or not.

[30] For example, in an exchange between Keith Baines and Colin Lenton-Smith in September 2001, Fujitsu denied it was in breach of a term of the Original Codified Agreement (concerning the roll out of pilots), but agreed to suspend its new keys pilot, saying itwould not recommence this unless it received a CCN. (POL00401662; POL00401661). This appears to have led to discussions about whether timings for calculating compliance should expressed afresh though a CCN after each 'major release' (POL00401660) and later a discussion about whether or not this particular CCNshould incur a new charge to POCL (POL00401659). Later correspondence in the Spring of 2003 illustrates negotiation

WITN03680200

47. The purpose of the '**Change Control Board**' (which I understand was also sometimes referred to as the **'Business Change Control Board**) was "*...to agree timescales for processing Change Requests* (*"CRs") and CCNs*"[31], to monitor and review reasons for the rejection of CRs and CCNs and to resolve questions as to whether particular changes would require an amendment to the contract via a CR or CNN, (a change amendment to the Codified Agreement).[32][33]

48. It is also my understanding that a range of other boards and forums also appear to have been established in 2000 that were not directly referenced or provided for in the Codified Agreement, but which still appeared to have had a monitoring function in so far as compliance with the provisions of that Agreement were concerned.

49. During the period between 1999 and 2006, it is my understanding that responsibility for monitoring and operational matters relating to the service review[34] of the Horizon system lay with the '**Business Service Management**' department (**"BSM"**), which sat within the Post Office Network unit (**"PON"**).[35] BSM[36] was responsible for, among other things, incident management, problem

---

between Mr Baines and Mr Lenton-Smith about whether particular CCNs should attract charges or not (POL00401658; POL00401657; POL00401656; POL00401655). I have viewed these pieces of correspondence in isolation, and so cannot provide any further information regarding the context of that correspondence or what occurred thereafter.

[31] Schedule A05 of the Original Codified Agreement, Schedule 5 of the 2002 Agreement and Schedule A3 of the Current Contract state that this is the document that formally alters the provisions of the Codified Agreement after a Change Request had been considered and agreed by both Post Office and Fujitsu.

[32] POL00399922

[33] As defined in the table detailing the purposes, scheduling and attendees of various boards in the Annex of Schedule A04 to the Codified Agreement.

[34] A service review would take place to consider the service levels provided for within the Codified Agreement, progress against those levels by Fujitsu and agree a proposal as to how to monitor and manage those levels going forwards.

[35] POL00393957. p.6. In this document, the Business Service Management department, as "*a dedicated function within the Post Office Network Unit that supports the automated (Horizon enabled) platform*".

[36] POL00393983 dated December 2000; POL00394054 dated February 2002.

WITN03680200

management, service review and performance.[37] I have had sight of examples of Operational Level Agreements and an associated Strategy Statement that make it clear that the review of reference data[3839] fell to BSM.

50. It appears from an SLA[40] dated 23 April 2001[41] that, following a commencement of an internal trial within the Post Office, the responsibilities of BSM were defined further to include:

    a. managing the interface with Fujitsu, in respect of ensuring that SLAs[42] are reported on;

    b. providing instructions that relate to Horizon for new and amended transactions, and monitoring and reporting on the impact of the introduction of such transactions;

    c. carrying out Incident and Problem Management in respect of Incidents and Problems that that arise in the operation of counter transactions;

    d. Managing the review of services across the automated network including the management of Fujitsu in relation to the provision of the Horizon

---

[37] POL00394060, dated 2002.

[38] Reference data enables applications to be customised using data driven changes as opposed to code changes, thereby providing a mechanism for implementing operational business changes more quickly and reliably.

[39] SGO reference data changes are a change/update to parameters that drive various elements of the Horizon platform (such as pricing data etc). Fujitsu receives these changes from Post Office and applies them to the live system.

[40] SLAs were agreements that set out the standards of service Fujitsu were required to meet in relation to different aspects of the services to be provided pursuant to the main agreement.

[41] POL00393987, 'Service Level Agreement between Internal Account Management and Business Service Management'. A further version of this document (dated 29 June 2001 v.1.0)extended the trial to September 2002.41 These trials were underpinned in March 2002 by a set of formal (but internal) Service Level Agreements and Requirements Catalogues for the Business Service Management unit and extended to new products in the Business Services Management & Network Banking Integration programme of work to catalogue the new requirements placed on the Business Service Management unit.

[42] Service Level Agreement Schedule A01 of the Original Codified Agreement, Schedule 1 of the 2001 Agreement and Schedule 1 of the Current Contract state that this is the quantifiable, measurable standard required by Post Office for a given service as agreed by Post Office and Fujitsu.

WITN03680200

services as defined within Schedules E1 to E9 of the Codified Agreement, *"this will include the analysis of performance data and the sourcing/provision of appropriate PON business information"*;

e. Managing and supporting *"a hierarchy of Service and Operational Review forums, covering the full range of the Horizon Service, as well as, subject to business approval, other services and processes within the end to end process of which Horizon forms a part;"*

f. Providing *"standard reports and, on request, ad hoc reports, detailing the performance of the Horizon Service;"*

g. Producing and maintaining *"the client impact scoring matrices on behalf of Internal Account Management Team ("IAMT") in relation to all POCL/ICL Pathway Service Level Agreements and any others that may subsequently be added to the Business Impact Model at a future stage;"*

h. Managing *"a process focused on Horizon Outlets, whereby proposals for improvements to any aspect of the Horizon Service can be raised, and will be assessed, and where appropriate developed and implemented."*

51. It is therefore my understanding, following my review of that SLA, that the function of BSM was to discharge the overall **Service Management Framework**. The first Service Description of this Service was issued on 31 December 2002[43], which coincided with the introduction of the 2002 Agreement. However, I have noted that the phrase was used but was not defined in the Original Codified Agreement. It is my understanding that this

[43] POL00394118

WITN03680200

Service integrated several other services at meetings of the Service Management Forum.

52. The Service Management Framework defined *"the strategy, policy and principles that govern the development of Service Management process models and enable co-operative Service Management by POCL and ICL Pathway"* and was made up of the following disciplines:

    a. Incident Management;

    b. Problem Management;

    c. Change Management;

    d. Service Configuration Management;

    e. Business Continuity Management;

    f. Service Review; and

    g. Performance Reporting and Management Information[44]

53. It was stated within the Service Management Service: Service Description Contractually Controlled Document ("CCD") that the purpose of the service was essentially to monitor manage and maintain the delivery of Operational Services.[45] It is my understanding that the Service Review part of this service (which I will describe further below) that had responsibility for identifying and reporting of BEDs, whereas the actual rectification and fixing of any identified BEDs would be carried out as part of the wider Service Management Framework described above, as part of the incident and problem management process.

[44] POL00393882
[45] POL00400131

WITN03680200

54. The **Service Review Framework** which was one aspect of the Service Management Framework that I have referred to above established the *"definitions and policies that have been agreed for the provision of reviews of the Horizon services by Post Office Counters and ICL Pathway."* The arrangements were, as I understand it, underpinned by a series of Framework documents which were settled between Fujitsu and Post Office. Essentially, as I understand it, the purpose of the Service Review Framework was to monitor Fujitsu's compliance with requirements to fix identified problems within specified timeframes. These were periodically reviewed and updated. As a result, multiple versions of each document exist.[46]

55. By November 2000, BSM had established formal sub-forums to facilitate ongoing monitoring of Horizon and for there to be an iterative process of improvement of Horizon in order to meet its responsibilities as defined above.

56. A document entitled *"Service Management / High Level Process Description / Service Improvement"*[47] dated 14 November 2000[48] illustrated the structure of the forums in place,[49] which shows that there were:

    a. **"PON Internal Meetings to address business issues:**

    b. **Horizon Programme Board; Horizon Evaluation Review Forum;**[50]

    c. **OBC**[51] **(Network) Forum;**

    d. **OBC (Product) Forum"**

---

[46] POL00398160
[47] This document was drafted by Paul Martin (Process Design Manager) and was authorised by Harvey Skipsey (Head of Business Service Management).
[48] POL00393957
[49] POL00393957, p.28
[50] All other documents that I have reviewed that refer to this Forum suggest that the meetings were joint with Fujitsu.
[51] OBC was an acronym for "Operational Business Change".

e. **"ICL Pathway / PON cross-domain[52] meetings to address Horizon cross domain issues:**

f. **Horizon Commercial Forum;**

g. **Horizon Service Review Forum;**

h. **Reference Data Forum;**

i. **Transaction Data Forum**

j. **IRERF Forum [Incident Reconciliation Exceptions Review Form]**

k. **Problem Management Forum**

l. **AP forum [Automated Payments Forum]**

m. **LFS Forum [Logistics Feed System]"**

n. **"ICL Pathway Internal Meetings**

o. **ICL Pathway internal review forum**

p. **Internal Operations Meetings"**

57. However, whilst reference was made in that document to the meetings of the Horizon Evaluation Review Forum being internal within Post Office, the other documentation that I have reviewed for the purposes of preparing this statement refers to the fact that the meetings were joint with Fujitsu.[53] The focus of these meetings was referred to as being *"similar to that of the Horizon Service Review Forum to assess the impact of NRO [national rollout] on the business"*.[54] In 2001, it is my understanding that the Forum's focus changed as the rollout of Horizon to outlets neared completion. As a result, it is my understanding that the Forum was concluded and replaced by the **Automated Services Forum**.[55]

[52] I understand cross-domain to mean in this context, cross IT system meetings between Post Office and Fujitsu.
[53] POL00393987
[54] POL00393957
[55] POL00394001

WITN03680200

58. The Horizon Service Review Forum's meetings (between POCL, Fujitsu and the Department of Social Security) were held to review the overall performance of Fujitsu's systems and services. It is my understanding that the forum reviewed all services provided by Fujitsu under the general umbrella of the Horizon system. Meetings are recorded as having included discussion of a variety of Fujitsu's contracted services, including the review of *"major incidents and/or significant outstanding problem," "quantitative and qualitative assessment of services"* and *"developing and monitoring of service improvement initiatives".*[56]

Service Review

The approach to Service Review

59. It is my understanding that "**Service Review**" was the central internal measure that Post Office used on an ongoing basis to monitor all of the contractual obligations that Fujitsu had pursuant to the Codified Agreement. This included the obligations that related to sections 2(a) and 2(b) of the Rule 9 request.

60. In the Codified Agreement, the services that Fujitsu supplied ("the **Services**") were divided into categories.[57] These Services were then broken down – and each of the sub-categories had its own SLT ("the **'Service Level Sub-**

[56] POL00393875

[57] In the Original Codified Agreement, the Services that Fujitsu provided were broken down into: the automated payment service (Schedule E1 – E9), Electronic Point of Sale Services (Schedules F1 – F9), POL Infrastructure Services (Schedule G1 – G11), OBCS (Schedules H1 – H9) and the Logistics Feeder Service (K1 – K9)
In the 2002 Agreement, the Schedules that Fujitsu provided were broken down into: the Operational Services (Schedule 19), the Development Services (Schedule 20), the Business Continuity Services (Schedule 1), the Branch Hardware Implementation Services (Schedule 23), and the Banking Implementation Activities (Schedule 24)
In the Current Contract, the Schedules that Fujitsu provided were broken down into Development Services (Schedule B1.1 – B1.3), HNG-X Services (Schedule B3.1 – Schedule B3.3), Transfer Services (Schedule E)

WITN03680200

Obligation") which was monitored in isolation. Therefore, when an SLT related to a Service Level Sub-Obligation that, in turn, related to obligations relevant to sections 2(a) and (b) of the Rule 9 request, the ongoing Service Review of that SLT represented an important way in which Post Office could monitor Fujitsu's contractual adherence to the relevant contractual obligations.

61. A Service Level Sub-Obligation that relates to the relevant contractual obligations can be found within most Services because of how broadly BEDs could affect those services (for example, a BED may have caused a failure in relation to the automated payment service). There was not a separate or distinct category of SLTs for the identification or rectification of BEDs.

62. I will use the SLTs relating to the Horizon System Helpdesk (**"HSH"**), which was part of the Infrastructure Service, for the purpose of illustrating how the SLTs were designed to work in practice. I have chosen this SLT as an example because the Horizon System Helpdesk was the *"the first point of contact for Customers of the POCL Services"* experiencing problems (which would include errors that might be caused by BEDs) according to Schedule G01 of the Original Codified Agreement. It is also my understanding that customer reporting was the way that most BEDs were identified and so the operation of this SLT directly relates to the relevant contractual obligations as defined in section 2(a).

63. In the provisions of the Original Codified Agreement that deal with the HSH, the Service Sub-Obligation to repair a problem (which may or may not have been caused by a BED) in a given time ("**Time to Repair**") was summarised in the following table:

WITN03680200

Class Call	Local Non-Remedial	Local Remedial	Intermediate Non-Remedial	Intermediate Remedial	Remote Non-Remedial	Remote Remedial
'A' Priority	4 hours	6 hours	6 hours	9 hours	8 hours	12 hours
'B' Priority	8 hours	10 hours	10 hours	15 hours	12 hours	24 hours

64. This table demonstrates that when a problem or incident was reported to the HSH it was categorised by *"Priority"* and *"Type of Branch"* as follows:

a. **Priority:** '*A Priority*' problems were those that impacted on all of the counters in a Post Office. '*B Priority*' problems were those that impacted on one of the counters. In reality, it was unlikely that a problem would impact only on a small number of counters when they were running the same version of Horizon. It is my understanding that the division between Priority A and B problems is likely to happen where localised outages impact on counters in a particular geographical area.

b. **Type of Branch:** a branch was considered to be Local, Intermediate or Remote based on its geographical location. Which category it fell into was determined by postcode in the CCD 'Definition of Remote and Intermediate Locations.'[58] CCDs are defined in the main agreement[59] as either documents referred to as CCDs in the main agreement, listed as CCDs in a document titled *"Contract Controlled and Referenced Document List"*[60] or which can only be amended through the Change Control Procedure.

[58] POL00401640
[59] 2002 Agreement, v1.0
[59] POL00393915

WITN03680200

65. The SLT for Time to Repair differed depending on what categorisation it was given.

66. The table also differentiates between '*non-remedial*' and '*remedial*' timescales. The non-remedial column represents the SLT. For example, taking a category B problem in a local branch- if the time to repair exceeded 8 hours, this was deemed to be a failure of the SLT – which meant that Fujitsu had failed to meet their associated contractual obligation. The columns that contain the phrase "*remedial"* highlight the threshold at which point a remedy would become available –which I will discuss and explain further in my response to question 3(d) below (see paragraph 369 onwards). In other words, if after the expiry of 8 hours from when the problem was reported, there was a failure to meet an SLT, a remedy then became available after 12 hours.

67. Due to the sheer volume and complexity of SLTs within the period that is the subject of the Rule 9 request, I have been unable to identify every SLT that may relate to a relevant contractual obligation. However, I am able to confirm that after the 2002 Agreement, the SLTs for all of the Service Level Sub-Obligations were summarised in the CCD entitled *"Service Level Targets for Horizon Services"*, which extracts the Service Levels from the Codified Agreement and explains them.[61]

Service Review Structure

68. Post Office implemented a Service Review Structure to monitor the degree to which the SLTs for Service Sub-Obligations were being adhered to. It was in place between 1999 and 2006 in various stages of completeness. In April of

[61] POL00400777

WITN03680200

2000, an Internal Audit of the HSH found that documents relating to the Service Review Framework were incomplete and recommended that their "*content be finalised, agreed, approved and deployed without delay*".[62] It appears that it was finalised at some point thereafter between 2000 and 2002. However, I have not seen any finalised versions from this period. It is my understanding that it[63]was subsequently further[64] updated.

69. The most definitive version of a document which describes the Framework is a Service Review Framework Final Draft from March 2002[65] which appears to have been prepared while the revision process was ongoing. This document stated that the Framework had three levels:

    a. The Senior Management Level (Section 1)

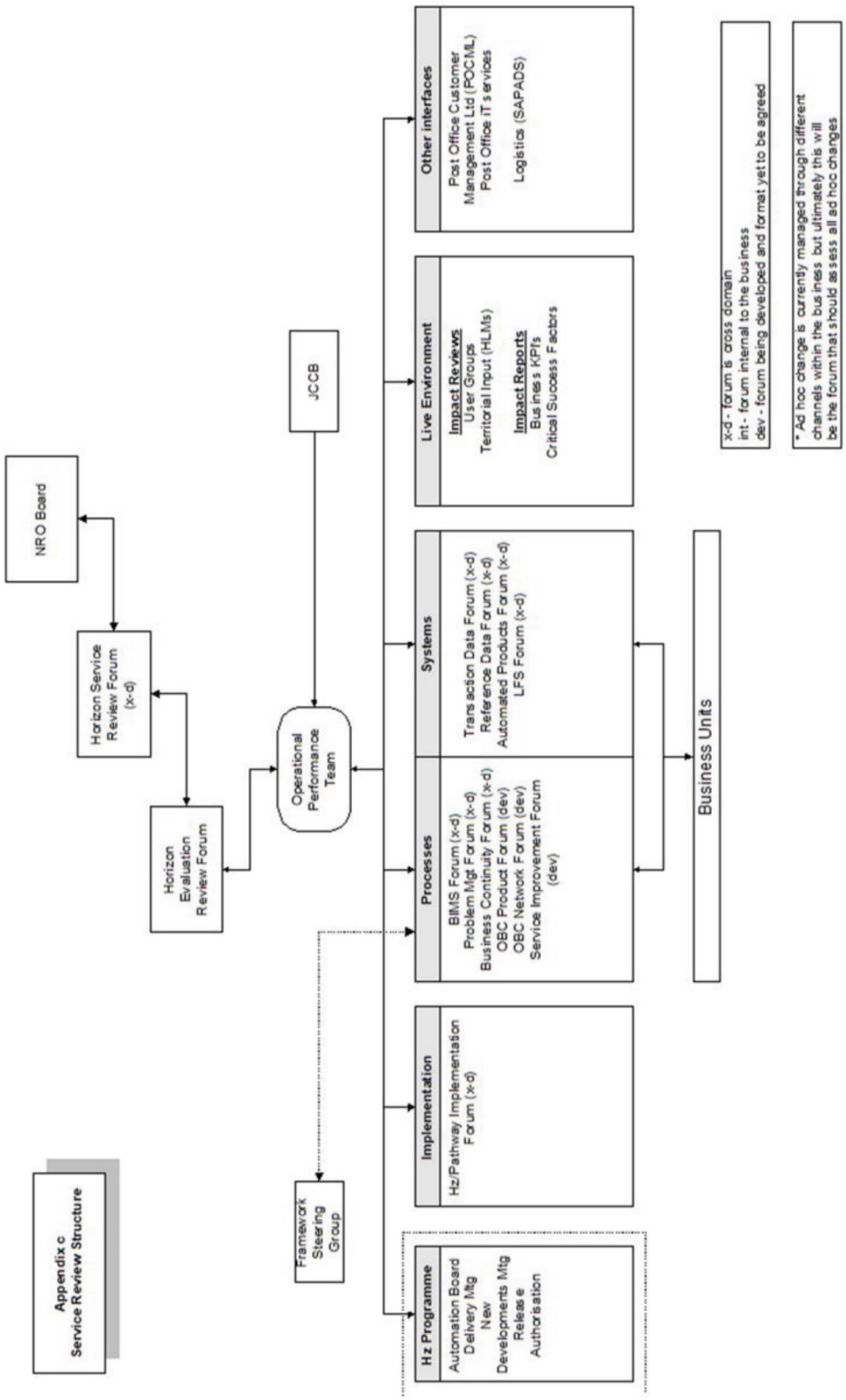
    b. Operational Level (Section 2)

    c. Business Unit Level (Section 3)

70. They were structured as is shown in the diagram below:

[62] POL00393913
[63] POL00394097
[64] POL00394098
[65] POL00394064

WITN03680200



WITN03680200

The Senior Management Level

71. The Board with the overarching responsibility for Service Review was detailed in the *'Governance'* Schedules of the Codified Agreement.

72. In Schedule A04 of the Original Codified Agreement this Board was known as the '*Service Review Board'* or the *'Horizon Service Review Board'.* Its responsibilities were:

    a. To review Fujitsu's performance against contracted service levels

    b. To agree remedies payable arising from any failures to meet service levels (this process is explored further in the response to question 3(d) of the Rule 9 request below at paragraph 364.)

    c. To monitor and review operations of operational business change processes.

73. In Schedule 4 of the 2002 Agreement, the Board became the Service Management Forum[66] or the 'Horizon Service Management Forum' and was also known as the 'Horizon Services Review Forum'. The responsibilities of this Board appear to have been similar to, but arguably wider than, those of the 1999 Service Review Board. The responsibilities that would appear, based on my understanding to have related to the relevant contractual obligations in relation to sections 2(a) and (b) are:

    a. Reviewing performance against contracted service levels and agreeing remedies payable (if any).

[66] This is implied by the progressive drafts of the 'Service Management Service: Service Description', in which Section 3.3 transitioned from 'Structure of Service Review Board' into 'Structure of Service Management Forum' between Version 0.1 issued on 1 December 2002 and Version 1 issued on 31 December 2002 (in alignment with the new version of the Codified Agreement.

WITN03680200

b. Reviewing the operational reliability of Branch Infrastructure and considering/recommending remedial courses of action (e.g. full or partial technological refresh or service level relief).

c. Resolving operational issues including, but not limited to, those arising from non-conformance to contracted service levels

d. Ensuring continuous improvement in the ongoing/steady state/business as usual Service Management environment.

e. Reviewing future change plans to ensure the live environment was adequately prepared.

f. Capacity management.

g. Monitoring and reviewing operations of Operational Business Change processes.

74. In Schedule A2 of the Current Contract, the Service Management Relationship was the body with responsibilities for Service Review. However, I have been unable to identify which precise Boards were set up by this Relationship (see paragraphs 141-143).

75. During the 2000 – 2006 period, it is my understanding that the Service Review Board and the Service Management Forum (together '**The Horizon Forums**') were the "*top level formal review between POCL and ICL Pathway*"[67] and had the express purpose of "*reviewing performance against contracted service levels and agreeing remedies payable (if any)*".[68] They appear to have been the key forums monitoring Fujitsu's compliance with the relevant contractual obligations because they monitored Fujitsu' adherence to all contractual terms.

[67] POL00393913
[68] 2002 Agreement, Schedule 4, Annex 1

WITN03680200

76. The Horizon Forums appear to have been attended by members of both Post Office and Fujitsu, but the frequency of their meetings is unclear. Schedule A04 of the Codified Agreement provides for some of the attendees at these meetings, specifically the Head of Service Management and Meeting Secretary and others at POL's discretion. However, version 5.0 provided for additional attendees including the Service Operations Manager and the Head of Business Service Management.

77. Contractually, the Original Codified Agreement stated that the function of the Service Review Board was to meet monthly in Schedule A04; although a meeting referred to as the Service Review Meeting was to occur quarterly.[69] In Schedule 4 of 2002 Agreement, it was also stated that that the Service Review Board meetings were monthly.

78. I have had sight of a meeting schedule for a Service Review Board meeting from 1999 which confirms that the meetings were monthly in this period.[70] This is reinforced by meeting minutes that I have also seen. In documentation that I have reviewed from 2002, it appears that the meetings were less frequent and occurred on a bi-monthly basis.[71] However, by 2003, based on the documents that I have reviewed, they seemed to have met monthly again.

Sources of Information for Service Review at the Senior Management Level

79. The Horizon Review Forums appear, based on the documentation that I have reviewed for the purposes of preparing this statement, to have received reports

[69] Original Codified Agreement, Schedule E05, Paragraph 3.2.1
[70] POL00394091
[71] POL00394015

WITN03680200

in relation to the services provided by Fujitsu pursuant to the Codified Agreement from two main sources. These were:

a. Reports provided as part of the Management Information Service – in particular the Service Review Book (examples of which I have referred to below between paragraphs 81-84).

b. Operational Forum Reporting (see paragraph 94 for Operational Level section).

Management Information Service Reports and the Service Review Book

80. Throughout the contractual term, Fujitsu were contractually obliged to report to Post Office on the degree to which they were meeting the contractually stipulated SLTs.

81. The central means of doing so appears to have been through the Service Review Book (also known as the Service Management Report), which Fujitsu was contractually required to provide on a monthly basis under Schedule A06 Paragraph 4.2 of the Original Codified Agreement, Schedule 15 Paragraph 2.4 of the 2002 Agreement, and Schedule B4.4, Paragraph 2.3 of the Current Contract.

82. A document entitled '*The Management Information Service: Service Description"* (which I will summarise as **"The MIS: SD"** for ease of reference), defined the contents of the Service Review Book and explained its purpose. It stated it was the *"primary input into the Service Management Forum on performance against SLTs".* It also detailed the other monthly reports that Fujitsu was obliged to provide.

WITN03680200

83. It is my understanding that 8 versions of this document were produced during the course of the relevant period and that the content of the Service Review Book differed across those versions.

84. The Service Review Book does not appear to have materially changed between the Codified Agreement coming into force and 18 November 2004. Although version 1 of the MIS:SD was issued on 20 December 2002 (over three years following the Codified Agreement), it referred to content that had been in place since 1999. The document, during this period, was structured, in summary, as follows:

a. SLT data – which was the comparison of Fujitsu's performance against the SLTs.[72]

b. Management summaries detailing the highlights of the last month's service delivery.

c. A high- level review of each of the supplied services.

d. Volumetric data.

e. A high-level review of problem management and cross domain problem status.

f. A high-level review of release management including releases delivered.

g. Annexes identifying Engineer Service Failures attracting remedies (including liquidated damages), with the following details relating to each failure: *"Incident reference"*; "*Degree of failure"*; *"Brief explanation of the incident"*; *"Explanation of the cause of failure"*; *"Action planned to*

[72] POL00394102. The SLTs were broken down according to the following services in this period: Helpdesk Service, System Service, Data Service, Transaction Service, Training services, implementation and rollout and LF Service.

WITN03680200

mitigate further failures." However, I have been unable to locate any such annexes in the Service Review Books and packs that I have reviewed for the purposes of preparing this statement.

85. It is my understanding that the key section of this document, in relation to Service Review, was SLT Data ('A' above) – which evidenced the degree to which Fujitsu reported to Post Office that they had met their SLTs. I understand that Fujitsu would classify its adherence to the relevant 'Service Level Sub-Obligation' using the following colour coding:

    a. Green: indicated performance on the part of Fujitsu that was above the level required.

    b. Yellow: indicated a one-off failure with either an action plan in place or not required.

    c. Red: indicated a repeated failure.

86. An example of this colour coding system in practice can be found in the 2001 Service Review Book in which the HSH SLTs for Time to Repair (see paragraph 63) were tracked as follows:

WITN03680200

Oct00	Nov00	Dec00	Jan01	Feb01	Mar01	Apr01	May01	Jun01	Jul01	Aug01	Sep01	Call to Resolution (Remote)	MAT	TRT	Comment
100.0	71.4	87.5	100.0	100.0	100.0	100.0	100.0	100.0	60.0	100.0	100.0	Hardware/Network Priority A - 8 hours Non-Remedial	95%	N/A	
	78.5	Q4		96.6	Q1		100.0	Q2		83.3					
96.2	90.7	93.3	98.3	100.0	100.0	98.0	100.0	100.0	100.0	100.0	100.0	Hardware/Network Priority B - 12 hours Non-Remedial	95%	N/A	
	90.8	Q4		99.2	Q1		99.1	Q2		100.0					
100.0	86.7	87.5	100.0	100.0	100.0	100.0	100.0	100.0	60.0	100.0	100.0	Hardware/Network Priority A - 12 hours Remedial	100%	N/A	
	92.9	Q4		96.6	Q1		100.0	Q2		83.3					
100.0	97.5	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	Hardware/Network Priority B - 24 hours Remedial	100%	N/A	
	98.6	Q4		100.0	Q1		100.0	Q2		100.0					

WITN03680200

87. The central column in white – with the heading '*Call to Resolution' (Remote)'* mirrors the SLTs for '*Time to Repair (Remote)'* detailed in the Codified Agreement – which are detailed in the table above: specifically: 8 Hours to resolve Priority A calls and 12 hours to resolve Priority B calls. As stated above, the *'Remedial'* timescales will be discussed in my response to question 3(d) below (see paragraph 372 onwards below).
88. The column entitled **'MAT'** (Minimum Acceptable Threshold) shows the percentage of cases that Fujitsu needed to meet the SLT in – so, Fujitsu needed to repair a Priority A fault at a remote branch within 8 hours 95% of the time.
89. The left-hand side of the table, containing the colour coded squares, shows the percentage of the time that Fujitsu met the SLT in the given month. For example, September 2001 is coloured green because it was above the 95% level. However, July 2001 is coloured yellow because Fujitsu only met the expected level for the time taken to repair an issue in 60% of cases. I have not been able to establish what, if any, tools were available to Post Office to monitor if Fujitsu was accurately reporting its performance in the Service Review Books.
90. I will discuss the columns on the right hand of this table (entitled MAT and TRT) further in the liquidated damages section (see paragraph 372 onwards).
91. As subsequent versions of The MIS:SD were developed, Fujitsu's reporting requirements also changed. This had an impact on the extent to which Post Office monitored certain contractual obligations. I have detailed below the version changes that contained provisions related to the relevant contractual obligations (and the associated impact on Post Office's monitoring of those obligations) below.

WITN03680200

a. It is my understanding that, in **Version 3**, issued on 8 July 2005, an important change was introduced in that Fujitsu were obliged to report all failures against SLTs as well as Engineer Service Failures under 'G' above. However, despite seeing numerous references to this annex in documents that I have reviewed for the purposes of preparing this statement, I have not been able to locate it to date.

b. In **Version 4** (for which the official version title was reset to **'1'** (i.e. Version 1) as it coincided with the Release of the 2006 Codified Agreement), issued on 24 August 2006, '*Summary Service Overviews',* were added to the Service Review Book. These augmented the 'High-Level Reviews' for each of the Services that were required pursuant to Version 1 released on 20 December 2002 ('C' Above) by adding further graphs that drew out key information.[73] In addition, a more extensive narrative summary was added for each of the Services' sections.

c. I have reviewed a document[74] which stated that the Service Management Portal contained the following management information: Real time Service Monitors:

   i. SLT information – provided on a daily, monthly and quarterly scale

   ii. Registers of Customer Service Improvement Proposals

[73] The SLT Performance by SLT Group showing the overall number of SLTs falling into the red, amber or green category. The SLT Performance by SLT group for the reported month when compared against the 12-month average. This would be labelled either– 'Up' if it was higher or 'Down' if it was lower. The monthly performance of services delivered to branches– as opposed to just those services delivered to Post Office. The Customer service scorecard compiled of customer feedback– which would also be compared against the 12-month average and be labelledeither – 'Up' if it was higher or 'Down' if it was lower.
74 POL00395270

WITN03680200

iii. The Service Review Book

iv. Major Incident Reports

v. Weekly Service Management Report

vi. Operational Business Change Schedules

vii. OCP Information and Schedules

d. The SLT information described above gave Post Office real-time access to the service level reporting of any SLT – and, therefore, it is my understanding that Post Office could check the status of Fujitsu's performance in relation to any Service Level Target that was relevant to the relevant contractual obligations within sections 2(a) and 2(b), at any time. In addition, Major Incident Reports were a key way through which BEDs were identified and Post Office had access to those on the Service Management Portal. Customer Service Improvement Proposals were a means through which Fujitsu could propose an improvement plan. However, it is my understanding that this was not a means through which the rectification of BEDs would be taken forward.

e. **Version 6** (the official title for which was **Version 3**), issued on 2 February 2010, removed the requirement for the following to be included in the Service Review Book:

i. Volumetric data ('C' above);

ii. A summary review of releases ('E' above);

WITN03680200

iii. Annexes that detailed where liquidated damages were payable for the month being reported on – or the details associated with them ('F' above);

iv. The customer service scorecard.

f. From the point at which Version 5 was issued on 5 November 2013, the Service Review Book only consisted of monthly SLT achievements compared against the data in relation to the preceding 13 months displayed in an excel spreadsheet. Management summaries formerly listed at 'B' were to be provided in separate documents. These changes remained in place as the CCD was not modified again until 7 January 2022.

92. The consolidated monthly reporting within the Service Review Book was further provided for as follows:

a. **Version 1, Version 2 and Version 3:** Network Banking, Automated Payments, Capacity Management;

b. **Version 4** (the official title for which was **Version 1**) and **Version 5 (**the official title for which was **Version 2**) and **Version 6 (**the official title for which was **Version 3)**: Banking and Related Services, Automated Payments

c. **Version 7** (the official title for which was **Version 4**)

93. It is my understanding that, through an analysis of the sources of Fujitsu management information that are described above, the Horizon Forums would review whether Fujitsu had fallen beneath the SLT for a given Service Level

WITN03680200

Sub-Obligation (which would include those that related to the relevant contractual obligations). As a result, it is my understanding that the Horizon Forums were a key measure which Post Office implemented to track and evaluate Fujitsu's compliance with the relevant contractual obligations, based on the reporting that was provided to it by Fujitsu.

Operational Level – Operational Level Review Forums

94. It is my understanding that, Operational Level Forums (which had an oversight role in relation to many areas of the Post Office business, and were the subject of extensive restructuring between 1999 and 2006) played an important role in monitoring and reporting on Fujitsu's adherence to Service Levels by monitoring and relaying associated information to the Horizon Forums during this period. It is my understanding though that they were not responsible for the direct monitoring of compliance by Fujitsu with the relevant contractual obligations but that their reporting assisted that monitoring by other Forums which I will detail further below.
95. It is my understanding that Post Office's Operational Level forums were restructured extensively throughout the 1999 – 2006 period due to organisational changes.
96. These forums were governed by Operational Level Agreements, the purpose of which was to *"underpin and support service levels as agreed in SLAs"* by *"describing how a service or system will operate at an operational level."* These were non-contractual documents.[75]

[75] POL00394060

WITN03680200

97. In 2002, the Operational Level Forums included a Problem Management Forum. It is my understanding that this forum discussed problems (which would have included BEDs or other service failures that are the subject of the relevant contractual obligations) and determine whether, as it discussed problems, to check if they warranted escalation to the Horizon Service Review Forum.

98. It is my understanding that these operational level forums would produce feedback forms that documented the level of service in the subject area that each forum focused on and included reference to the issues that needed to be escalated to the Horizon Forums that sat above them for review. For example, the Horizon Help Desk had an Operational forum in early 2000[76] which I understand was a key way through which Post Office was alerted to malfunctioning software.

99. By way of example, the Live Environment Forum produced a periodic report entitled *"Horizon Programme / Business Service Management / Management of the Live Environment"*[77], which was referred to as the 'MoLE Report' and was circulated to a designated group of recipients.[78][79] I have only been able to identify one such report. It appears that the purpose of this report was to provide information in relation to, by way of example:

    a. *"(i); the management of the live environment and the effects of Horizon on individual business units which would be an internal Post Office*

[76] POL00393913
[77] Versions of this document have been recovered as follows: March 2000 (no. 31) POL00393787; April 2000 (No. 32) POL00393905; May 2000 (no. 33) POL00393795; June 2000 (also numbered no. 33) POL00393805; July 2000 (also no. 33) POL00393817; August 2000 (no. 34) POL00393829; September 2000 (no. 35) POL00393949, September 2000 (no.36) POL00393917.
[78] POL00393906
[79] POL00393904 (email)

WITN03680200

organisational grouping such as the finance team. The commercial team or the branch support team;

b. *(ii) critical success factors (CSFs) which were intended to highlight the impacts on areas of key performance as defined by business units; and*

c. *(iii) performance statistics for the Horizon System Helpdesk (HSH and Network Business Support Centre (NBSC) to provide visibility of potential problems."*

100. Other sections of the report detailed problems which had been open for 6 months or more and provided a number of specific examples which I have detailed in the bullet-pointed section at the end of this paragraph. However, as has been the case with a number of other documents that I have reviewed and referred to in this statement, I have reviewed this report in isolation. As a result, I am not able to comment on the context surrounding the examples that are set out below or what, if any, further actions were taken as a result:

a. *"Receipts and payments do not match ON Migration week … 24/05/1999 - 30/04/2000 PON are continuing to identify a way forward for progressing these problems and should conclude their strategy by the end of May. It has become clear that there is nothing within the contract that can enforce ownership to Fujitsu, therefore any changes will need to be funded by PON. Given that 95% of the incidents are still attributable to migration which has approx. 14 months to go, it is envisaged that this will become a 'known error'."*[80]

[80] A known error would be placed on a Known Error Log (KEL) when the root cause of a problem had not been identified or repaired, but there was a workaround that had been developed. The log was

WITN03680200

b. *"Receipts & Payments don't balance AFTER migration … 04/05/2000-31/05/2000… PON are continuing to identify a way forward for progressing these problems and should conclude their strategy by the end of May. It has become clear that there is nothing within the contract that can enforce ownership to Fujitsu, therefore any changes will need to be funded by PON. Given that 95% of the incidents are still attributable to migration which has approx. 14 months to go, it is envisaged that this will become a 'known error'."*

c. *"Contingency for system failure when balancing Jonathan Rogers28/09/1999- 04/05/2000Workshop to review proposed process - 16/05/00"*

101. It is my understanding that another example of an operational level forum relevant to the relevant contractual obligations that played a role in the monitoring of the relevant contractual obligations was the Post Office Network Executive Committee (**"PONEC"**). In 2000, the Committee received a package of documents which highlighted failures associated with the Horizon rollout. One of those documents, by way of example, was, an Update Paper report that was produced on 17 May 2000. This report which noted failures during the national rollout in the form of including an inability of frontline employees to deliver Horizon to the required standards.[81] A Performance summary was generated which described Fujitsu's performance over the previous year was

available for consultation by staff at the SSC who could use the workaround that was described in their advice to customers who made calls to the helpdesk.

[81] POL00393898. Attendees at the PONEC meeting were David Miller, Alan Barrie, Tim Thorpe, Dave Smith, Peter Turgoose, Eric Logan, John Main and Jon Millidge.

seen as poor on account of their service failures and failure to achieve key deliverables.[82]

102. I have not been able to identify any further examples of similar meeting notes (or associated documents) following the examples that I have referred to above, so I am unable to provide further assistance to the Inquiry in relation to the way in which the concerns that were raised were ultimately managed thereafter.

Testing and acceptance requirements

103. From the commencement of Post Office's contractual relationship with Fujitsu (with 28 July 1999 being the date of the Original Codified Agreement, as I have detailed above at paragraph 18), it is my understanding that measures were included into the Agreement that a given project or change to the Horizon system was monitored through testing, a condition imposed under Version 1, Schedule G01, Paragraph 5.3.3.3 of the Codified Agreement.[838485]

104. It is my understanding that the testing regime was comprised of the following:

a. Joint Testing: A joint testing process had been engrained in Post Office 's contractual relationship with Fujitsu since the preliminary agreements which, as I have outlined in my response to question 3(a) (see paragraphs 16-17) preceded the creation of the Codified Agreement in 1999. A *'Joint Testing Agreement'* dated 30 January 1998 stated that the aim of joint testing was to enhance the quality of the test and enhance Fujitsu's fault management.[86]

[82] POL00393900
[83] Codified Agreement 2006, Version 11, Clauses, Paragraph 9.2
[84] Codified Agreement 2006, Version 1, Schedule D1, Paragraph 15.2
[85] Codified Agreement 1999, Version 1, Schedule G01, Paragraph 5.3.3.3
[86] POL00393874

WITN03680200

b. Acceptance Requirements: Post Office defined criteria that needed to be met before products, software or services were released into the live environment[87], which were known as *'Acceptance Requirements'.* These applied to both new services provided pursuant to the Codified Agreement[88] and existing services that Fujitsu were updating or fixing.

105. The Acceptance Requirements and Acceptance Procedure for new Services introduced under the Codified Agreement were normally contained in a Schedule of the Codified Agreement. For example, Schedule A11 of the Original Codified Agreement described the Acceptance Requirements for CSR (the core, fundamental Horizon system).

106. These included specifications like secure operation in the case of service degradations[89], the use of audit trails, the preservation of system integrity, the use of encryption to prevent unauthorised access to or modification of data and the acceptable level of system resilience.[90] By doing so, Post Office put in place measures so that issues that were relevant to contractual monitoring which were taken into account before the system or update went live.[91] This appears to have applied to entire systems, such as the HNG-X Generic Acceptance Process[9293] and to smaller scale updates.

---

[87] The live environment was the Horizon system as used within Post Office branches.
[88] POL00397327
[89] Secure operation would relate to maintaining the levels of security around the Horizon infrastructure and applications. Service degradation may occur when, for example, security patches are not applied in a timely manner.
[90] POL00397087
[91] POL00397070
[92] POL00400363
[93] The HNG-X Generic Acceptance Process provided an agreed process to enable POCL to objectively confirm (known as a "Release Acceptance") that Fujitsu had fulfilled its obligations regarding the delivery of BAU Releases (those initiated by a customer change request, subject to commercial contractual terms and resulting in software application changes to the Live Post Office Estate). The process was managed via stage progression through Acceptance Gateways i.e. formal assessments of the required evidence. It also included mechanisms to rectify issues preventing the fulfilment of unmet

WITN03680200

a. **Quality Gates**: These were defined criteria that needed to be satisfied before the next stage of testing occurred. These were defined in the Codified Agreement[9495] as being based on objective entry criteria, drawn from generic checklists, to support the assessment of readiness, timeliness, worth and risk.

b. **Regression testing**: fixes for bugs, errors and problems would also be tested before they were implemented in the live environment to check whether they had an impact on existing functionality to make sure that the system was not adversely affected by the introduction of a change.

107. It was envisaged that before acceptance of the release of the software into the live environment, Post Office would conduct a final review to ensure that these various testing stages had been met.[96]

108. It is my understanding that the review was the responsibility of the relevant Release Authorisation Board, of which there were several. It is my understanding that attendees at the Release Authorisation Boards varied and may have been determined by the particular release that was the subject of a

---

Acceptance Criteria. The Generic process did not apply to all types of releases, including maintenance releases, the PODG Client Connection Service, and the Reference Data Management Service. Responsibility for managing the process rested with Acceptance Managers, who were either the Release Managers or specific individuals appointed by Post Office and Fujitsu. They agreed an Acceptance Plan which identified the timescales for provision of Acceptance evidence, which was usually determined by the Acceptance Method. The process would then involve Design Walkthrough, Document Review, Test and then Monitor.

[94] Current Contract, Schedule D1 (HNGX Design and Build), paragraph 15.2 which provided that"*Each test stage will have associated, documented quality gates (QGs) that will support the readiness review process to decide whether it is appropriate to enter or leave the stage of testing to which the QGs relate."*

[95] Original Codified Agreement: Schedule G01 (POCL Infrastructure Service Definition), para 5.3.3.3, 2002 Agreement: Schedule 20 (Development Services), Paras 2.1.2.2 and Current Contract: Schedule B1.3 (Development Services) Clause 5.4.3.

[96] POL00397066

WITN03680200

Board's meeting on a particular date.[97] Whilst I have not seen reference to something called a specific acceptance process, it is my understanding, based on the information regarding the process described above, that this was such a process. The acceptance process essentially amounted to a formal sign-off following the completion of testing, the review of test exit reporting, a review of any specific acceptance criteria (which would normally include things like defect thresholds) and then a final sign-off, which, at the time, would need to have been done by wet signature.

109. The Acceptance Requirements anticipated a level of system error and rolling rectification, and to that extent the scheme anticipated that some BEDs should not prevent system release and instead were to be recorded on a known error log ('**KEL**'). The KEL was used as a way of monitoring BEDs in the period between identification and determination being made as to whether it could be fixed. Once a BED had been remedied, it would be removed from the KEL. Individual BEDs could be escalated for inclusion on the KEL if they were not capable of being addressed prior to the proposed system release. Until around 2004, those individual BEDs were recorded as **'PinICLs'.**

[97] By way of example, at a meeting of the s.52 Release Authorisation Board on 15 March 2004, attendees included the Customer Service Director, the Operations and Support Service Manager, the Infrastructure Services Manager, the Service Introduction Manager, the Security Manager, the Project Manager, the Release Manager, the Business Continuity Manager, the Service Review Manager, the Contract Manager (Fujitsu Services), the Release Implementation Manager, the Release Implementation Support Manager and the Project Manager(POL00394339). At a meeting of a separate Release Acceptance Board in 2017, the attendees were recorded as being Post Office Project Manager, Post Office Business Analyst, ATOS Business Analyst, ATOS Project Manager, ATOS Test Manager, ATOS Architect, FJS Programme Management, FJS Development Manager, FJS Project Management, FJS Chief Architect, FJS Solution Architect, FJS Commercial, FJS Release Management, FJS Acceptance, FJS Operational Change, FJS Service and FJS Test Management (POL00400280).

WITN03680200

110. If the Horizon system was functionally defective as a result of a BED though, that would be classed as an unacceptable error that could prevent release (see also paragraphs 413-415 in which I confirm that this remains the position today).

111. The procedure for the escalation of individual BEDs to the KEL is apparent from documents associated with the release of software updates S50 and S60 around 2003 and 2004. Testing during mid-2003[98] identified certain areas that were being affected by PinICLs. Based on the documents that have been identified as relating to the matters that are the subject of this rule 9 request, it is my understanding that during this period lists of PinICLs were regularly sent by Fujitsu to POL on spreadsheets as part of the testing regime in anticipation of the software updates, with occasional reference to the need to escalate a particular issue to a KEL.[99]

112. The process is illustrated in internal POL emails from September 2003[100] where Graeme Seedall of POL IT directorate said:

"Some existing defects have been unearthed as a result of S50 testing - they will need to be added to the known error log. There will also be some unfixed defects on the new services (such as Bureau). We should get a fairly definitive view of the outstanding PinICLs at the end of testing next Friday - there would normally be a review to go through them".

113. The same email thread shows that by November 2003 it was identified that:

a) *"There is a "Deferred PinICL list" for S50 which explains the outstanding faults in business terms (we used to call it the Known Problem Register). A*

[98] POL00394195; POL00394198
[99] POL00394294; POL00394296, see cells F2 and F14
[100] POL00394310

WITN03680200

new version has just come out with a few additions from RVT and LRDP, also an explanation of the planned action."

b) *"There is a design log for each product which contains not just PinICLs and their workarounds but known design flaws, missing requirements etc."*

114. There was a discussion, within that same email thread, about which team or organisation should 'own' this document and I have not been able to establish how this was ultimately resolved. However, I have reviewed a subsequent email thread from February 2004 in which it was implied that ownership of this document may have sat with Network Support[101], and I have seen emails exchanged in July 2004[102] which suggest that the KEL process was maintained by Network Support and Fujitsu.

115. By 2004, PinICLs were referred to as PEAKS. I have had sight of an email from June 2004 in which Fujitsu proposed to POL that a list of "faults raised during S60 functional testing which may have a business impact" should either be deferred to a future release, or included in the KEL.[103] The list itself is entitled 'Outstanding Peaks from S60'.[104]It is my understanding from subsequent emails that I have seen[105] that POL intended that those incidents would then be handled by the Problem Management team, which is a process I describe below at paragraphs 123-129.

[101] POL00394322
[102] POL00394532
[103] POL00394501
[104] POL00394503
[105] POL00394503

WITN03680200

(b) The adoption of measures to rectify bugs, errors and defects in the Horizon system

2000-2002

116. As part of the review of documents that I have carried out for the purposes of preparing this statement, I have considered reports that were produced for the '**Problem Management Forum**' **(also known as the 'Problem Management Operational Review Forum')** which I have referred to above in paragraph 56 as one of the sub-forums to the Business Management Unit, which were set up from November 2000. This appeared to be the forum, prior to 2002, through which measures that were required to rectify BEDs, in the Horizon system or associated access issues or impact on branch accounts were discussed and agreed between Post Office and Fujitsu. Fujitsu were obliged to establish procedures like these under Post Office's Requirement 914 in the **Original Codified Agreement.**

117. A problem, for the purposes of this forum, appears to have been defined in the same way as set out below (see paragraph 123 under subheading *'Problem management'*). This definition would, as I understand it, capture BEDs and system errors.

118. The ways through which problems could be escalated to the Forum are detailed in the associated Terms of Reference [106] as being:

a. Problem management database reports

b. Service improvement proposals

c. Issues raised to the forum from the Post Office Network or ICL Pathway

[106] POL00393982

WITN03680200

d. Minutes and Actions of a previous meeting.

119. By way of example, a meeting on 16 November 2001, attendees received the following:[107]

a. a meeting agenda;[108]

b. a '3 month old Problem Report';[109]

c. a 'Problem Management Status Report';[110]

d. a 'problem co-ordinator matrix';[111]and

e. notes from the previous meeting[112]

120. I have reviewed the two status reports. In the report for August 2001, reference was made to how outlets (which would be Post Office branches) are *"...experiencing problems with daily and weekly cash on hand figures not matching up" and that the Horizon Project "are working on a communication to outlets"*.[113]

121. In the October 2001 report, it was stated, in summary, that:

a. the slow running of counter systems had been ongoing for a considerable length of time; and

b. the current Fujitsu fix was not currently fit for purpose and needed to be resolved before being released into the Horizon live system.[114]

---

[107] POL00178059
[108] POL00178060
[109] POL00178061
[110] POL00178062
[111] POL00178066
[112] POL00178065
[113] POL00394008
[114] POL00178062, p.6. *"Slow Running at Counters / The problem has been ongoing for a considerable length of time. The day to day slow running (navigating from screen to screen etc.) has been difficult to*

WITN03680200

2002 onwards

122. By 2002, it is my understanding that a formalised process for incident and problem management had been finalised to fulfil Fujitsu's obligation to remedy defects in the Horizon system under Clause 6.2 of the **2002 Agreement**.[115] The process was detailed in a document entitled *"ICL Pathway Problem Management Procedures".*[116] The respective incident and problem management processes, as defined in that document, are summarised below.

Problem management

123. Problem management was required where a problem (which was defined as *"an underlying cause that may result in incidents"*) caused an impact substantial enough to warrant action to eradicate it. This would capture BEDs and system errors.

124. The purpose of problem management was to identify and resolve the root cause of issues that would otherwise create incidents.

125. It is my understanding that these types of problems were raised by Post Office with Fujitsu's daytime Duty Manager. Duty Manager is a Fujitsu role.

126. The Duty Manager would then contact the person who had raised the problem (referred to as *"the originator"*). This could, for example, be a sub postmaster.

---

prove and could be user perception. However, the Adjust Stock & Slow Rollover has been known about since April. A fix was devised for the problem but a side effect of this was that the order of reports generated would be different. POL therefore said that the fix was unacceptable as it stood. Fujitsu began working on the side effect to the fix. This had the effect of making the fix 'bigger' in size to the system. The Counter_S10R_DELTA package, which contains the 'Slow running Adjust Stock/Balance snapshot' fix as one of its components was piloted on 30/10/01. The pilot offices were to be monitored over the balance period and if the fix proves successful, it will be released to the rest of the live estate - we are currently waiting for details of the success of the fix."

[115] POL00393981

[116] POL00393981

WITN03680200

The purpose of the Duty Manager making contact would be to better understand the issue and decide if it met the problem criteria, whether the issue was a Major Business Continuity Incident and who was best placed to act as the associated Problem Manager. It is my understanding that historically, this role would be taken by a Fujitsu employee but that, from approximately 2012 onwards, Post Office employees could also take on the role of Problem Manager.

127. A Problem Manager (who, in this example would have been a Fujitsu employee)[117] would be allocated to each problem on the basis of their knowledge, expertise, responsibility and availability. Their role was to ensure the problem was investigated and resolved and to provide progress reports.

128. Once allocated to a problem, the assigned Problem Manager would contact the person who had raised the problem. If the Problem Manager accepted that the issue was a problem, they would then pursue the *'acceptance routine',* which included checking Fujitsu's problem database for previous reports of the problem, recording supporting evidence and agreeing closure criteria and an update schedule. The Problem Manager would then develop an action plan, setting out actions to be taken by specific individuals in relation to the identification and resolution of the root cause of the problem and the monitoring of the solution applied.

129. Problems would be closed when the Problem Manager had determined that the problem could be closed. This would be, as I understand it, reported to Post Office by Fujitsu. The person who had raised the problem (which may have

[117] It is my understanding, by way of example, that, in 2012, Steve Bansal and Steve Gardiner, who were both Fujitsu employees, both held the title "Problem Manager".

WITN03680200

been a sub postmaster) would then be advised by the SSD that it had been closed.

Incident management

130. Incidents[118] that occurred with the Horizon system were, as I understand it, to be managed via function-specific help desks, the focus of which was to resolve incidents as quickly as possible and restore affected operations.

131. These helpdesks included the HSH, which dealt with *'System and Technical'* incidents and the NBSC which dealt with *'business incidents'.* BEDs would technically fall within the definition of System and Technical Incidents. However, it is my understanding from discussions that I have had with Post Office staff who were in post at the time, that postmasters would tend to call the NBSC with most problems that they encountered, which meant that BEDs could also be reported through the NBSC, even though a BED would not strictly fall within the definition of a business incident.

132. It is my understanding that incident management would usually involve an initial investigation (and possible deployment of a temporary procedure), evidence collection, identification of the incident's root cause and the development, testing, release and monitoring of a solution.

[118] POL00397084. The RGMA Customer Service Incident Management Process defined these as "*Any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service*".

WITN03680200

133. It is my understanding that Fujitsu would report to Post Office regarding instances of incident management as part of the Service Reporting packs that it was routinely providing.

Post Incident Review

134. In certain circumstances, a Post Incident Review would be carried out. The circumstances in which this might occur would be if there was a particular issue associated with the management of a particular problem or if such a review had been requested by a third party. I have not seen any documentation that provides me with further clarification as to who, in this situation, would be classed as a third party. I anticipate that it is likely that it would be a party that was not directly involved in the incident management process.

135. The Problem Manager would be responsible for managing the Post Incident Review, which, as I understand it, involved producing a report to be used as a means for authorising closure of the problem with signed agreement, of each party. Any such post-incident reviews would, as I understand it, be reported to Post Office by Fujitsu as part of the Service Reporting packs that I have referred to above in relation to the reporting of the incident management process.

136. It is my understanding that the Fujitsu Problem Management Procedures document was regularly updated as the procedures evolved and that an equivalent process for incident management was finalised in 2006, entitled *'RGMA Customer Service Incident Management Process'.*[119]

[119] POL00397084

WITN03680200

2006 – 2013

(a) The identification, investigation, recording and reporting of (i) bugs, errors and defects in the Horizon IT system (ii) other network system failures or (iii) the impact of such events on branch accounts.

137. It is my understanding that the internal measures that were put in place to monitor Fujitsu's compliance with the matters defined in question 3(b) of the Rule 9 request (in so far as sections 2(a) and (b) of the Rule 9 request are concerned) can be summarised as follows in so far as the 2006-2013 period is concerned:

a. The introduction of new governance structures.

b. Routine testing.

<u>The introduction of new governance structures</u>

138. New governance structures associated with managing the contractual and operational relationship between Post Office and Fujitsu were introduced by Schedule A2 of the Codified Agreement in 2006, through what was described as the 'Service Management Relationship' which, as I understand it, was part of a wider programme to introduce 'Relationships' into the contractual governance structure.[120] It is my understanding that, pursuant to the Current Contract, more discretion was given to the newly created Relationships (in relation to the frequency of meetings, by way of example). Their creation also

[120] Codified Agreement 2006, Version 1, Schedule A2

WITN03680200

appears to have altered the role of the Boards (which I will describe further below). The Boards, which had previously (pursuant to the 2002 Agreement) been the subject of more stringent specifications and requirements were, following the creation of the relationships, defined as the delegated authorities of those relationships and appear to have been responsible for resolving any associated day-to-day operational issues that may have arisen.[121]

139. The four Relationships that governed the Codified Agreement were formed of various Directors or leads from both Post Office and Fujitsu, which were detailed in Annex 1 of Schedule A2 of the Current Contract. These four relationships were:

Systems Integration Partnership and Executive Relationship

140. It is my understanding that this relationship was intended to monitor the overall success of the relationship between Post Office and Fujitsu, including the resolution of any disputes escalated for Executive review pursuant to the Dispute Resolution Procedure (as defined in Schedule A2 of the 2006 Codified Agreement) and monitor the performance of Fujitsu's obligations in connection with this Agreement. It appears to have operated at a relatively high level and was not concerned with whether or not Fujitsu was acting in compliance with the relevant contractual obligations.

Service Management Relationship

[121] Codified Agreement 2006, Version 1, Schedule A2, paragraph 3

WITN03680200

141. It is my understanding that Service Management was a day-to-day function of managing the relationships with teams responsible for the delivery of the service. It was also a process through which to, by way of example:

a. review network performance;

b. review operational reliability of Infrastructure

c. consider/recommend remedial courses of action (e.g. full or partial technological refresh or service level relief); and

d. resolve operational issues including, but not limited to, those arising from non-conformance to agreed Service Levels, among other important functions. It also was intended to have the ability to impose financial penalties, if Fujitsu failed to comply with the relevant contractual obligations. Any such financial penalties would be in the form of *"Service Credits"*, which were referred to in the contract as *"liquidated damages"*.

142. This forum was intended to meet formally on a monthly basis[122] . The monthly meeting was equivalent to that of the former Service Review Board. The meetings would discuss matters such as what fixes needed to be developed and the associated timescales.

143. The information that was provided to the Board would, as I understand it, have been created and generated by Fujitsu and would have been provided in the form of a Service Management or Performance Report (which was a more substantial version of the former Service Review Book, although it was still prepared on a monthly basis).

[122] Codified Agreement 2006, Schedule A2– 'Governance'

WITN03680200

Commercial Relationship

144. It is my understanding that the purpose of this Relationship was to manage and administer the Codified Agreement, agree amendments to it subject to the Change Control Procedure, perform first level escalation for disputes, whether about the interpretation of the Codified Agreement itself, or about other matters such as invoices. It was also intended to monitor, review and report on events and progress and issue resolution in respect of market testing.

Programme/Release Relationship

145. It is my understanding that the purpose of this relationship under Schedule A2, Paragraph 4 of the 2006 Agreement, was to provide a governance structure for the introduction of each new programmes or release (which would be a new release of counter software elements of Horizon which may contain new functionality or updates to existing functionality, including fixes for BEDS) by creating three interlinked boards for it:

a. Programme and Release Boards had the responsibility of overseeing the development of programmes and releases according to time, budget and resource. They would manage new Horizon projects and review and resolve any operational issues that arose during the design and testing of new HNG-X programmes.

b. Acceptance Boards[123][124] were established for each release and were intended to meet as required to resolve issues arising from Acceptance activity and testing in accordance with the testing provisions of Schedule

[123] Codified Agreement 2006, Schedule A2– 'Governance'
[124] Codified Agreement 2006, Schedule A2– 'Governance'

WITN03680200

B6.3 of the Current Contract. Their purpose was to consider and resolve Acceptance disputes, Acceptance of the relevant Release and provide a recommendation to the 'Joint Release Authorisation Board' (see paragraph 145(c) below). An example is the HNG-X Acceptance Board,[125] which had the primary purpose of carrying out testing, measuring results against criteria and making a recommendation to the JRAB as to whether software could be released into the trial or into the Horizon system according to the stipulations of Schedule B6.3 of the Current Contract.

c. JRABs were established to agree the criteria and processes through which Releases would be authorised, following and acting on recommendations from the Acceptance Board, for release into field trial or live operation and carry out readiness reviews of stakeholders accordingly.[126]

d. It is my understanding that this Board would determine how and if to progress new solutions or changes to solutions through to the acceptance stage. This assessment appears to have been based on whether the project as stand-alone entity was ready to be implemented. This would necessitate considerations such as whether Fujitsu and Post Office were ready for the proposed release and that associated communications with postmasters and other internal stakeholders had

[125] Another example of such a Board was the HNG-X Acceptance Dispute Board, the purpose of which, I understand, was to settle Acceptance disputes.
[126] Previously this function appears to have been carried out by the Service Management Forum (a forum that included Post Office and Fujitsu members), which in accordance with the 2002 Agreement, would agree the processes by which releases would be authorised for release into field trial or live operation and would carry out readiness reviews.

WITN03680200

been completed. For example, they would decide when the Live Pilot and Live Monitoring of releases would commence.

e. They would receive recommendations from the Acceptance Boards as to whether the acceptance criteria had been met and if they had, as a result, a change to the Horizon system could be approved.[127]

Routine testing

146. Routine testing remained a feature of the contractual relationship from 2006 onwards as stated in Schedule B1.1 and Schedule D6 of the Current Contract.[128]

147. It is my understanding that non-functional testing (which is testing that is focussed on the performance of the system rather than the actual functions created (such as how long it takes for the system to respond to a button press against the question of whether Post Office has the right button to press)) was conducted. This testing was conducted by the Vulnerability Management Service[129], which worked to identify and reduce vulnerabilities in the HNG-X application. Although these tests were designed to identify potential problems arising from malicious digital attacks (such as Viruses, Trojans and Worms), vulnerabilities caused by configuration errors such as BEDs within software were also identified.[130] This is described in the document entitled 'HNG-X Architecture – Security Architecture' which was dated 24 September 2014.[131]

[127] Codified Agreement 2006, Schedule B6.3 – 'Acceptance Process'
[128] POL00396892, p.11
[129] It is my understanding that this was a service provided by Fujitsu.
[130] POL00398421
[131] POL00398421

WITN03680200

148. There were, as I understand it, a series of tests which were used, which I describe further below. I am able to describe the tests that were run, based on the information that I have been provided with to prepare this statement. However, I have not had sight of all of the test reports associated with those tests. This means that I am unable to provide the Inquiry with any useful level of detail as to the outcome of the tests.

149. The tests that were run were, as I understand it, as follows:

a. Quarterly **Approved Scanning Vendor scanning**[132] - This involved sample testing, carried out by an external party, of various aspects of the Horizon Architecture (such as routers, servers and wireless access points) for the purpose of ensuring PCI compliance (as described further above). The external party would produce a report detailing adherence, potential risks and suggested actions.[133]

b. **Penetration Testing**[134] was required pursuant to the 2006 Codified Agreement[135] and occurred either on an annual basis for all systems, or when a significant change to a specific system was implemented. The testing would use methods that might otherwise be used by hackers or those wishing to cause harm to a system in order to be able to identify faults or vulnerabilities in the system that required patching.[136]

c. **Disaster Failover Testing** occurred annually for the HNG-X systems and would involve a deliberate failure of the main production datacentre being engineered for the purposes of testing the resilience of the backup

[132] POL00398421
[133] POL00399608
[134] POL00396892, p.11
[135] Codified Agreement 2006, Version 1, Schedule B3.2, Annex 1, Paragraph 10.2
[136] POL00397485

WITN03680200

site.[137][138] It is my understanding that specific individuals would be assigned to plan and conduct the testing. For example, in 2008, Brian Pinder (Fujitsu) was given overall responsibility for testing the vulnerability of the PCI datacentres[139] while Mark Harvard (an external contractor from Computacenter) was instructed to develop the low-level test plan.[140]

150. If penetration or vulnerability testing identified a BED, the Network Security Management team assessed it and would either, as I understand it:[141]

a. approve an immediate/scheduled IOS fix as bug was already known to the project and the fix had already been tested and approved for deployment;
b. interrogate the relevant logs to gather more information;
c. notify the product supplier of the issue (using the standard support route);
d. escalate the issue within the organisation following the project procedures.

151. It is my understanding that significant findings from the testing were tracked via a remediation plan and technical risk assessment and could be escalated to the Information Security Management Forum ("**ISMF**") Risk Register.

152. The testing that I have described above was carried out in accordance with industry standards and, by way, of example, to ensure compliance with

[137] POL00401615
[138] POL00399707
[139] The Datacentres that held Payment Card Industry information.
[140] POL00396892, p.11
[141] POL00398165

WITN03680200

Payment Card Industry Standards ("PCI").[142][143][144][145][146][147][148][149] For example, the process for card payments through the Horizon System was benchmarked against the PCI council's recommendations.[150][151][152][153][154][155][156][157][158] Fujitsu were also required to demonstrate their adherence to PCI standards in the provision of the Horizon service to Post Office.[159] It is my understanding that sometimes, Post Office utilised the formal CCN procedure to make it a contractual term for Fujitsu to meet these specifications.[160]

153. Post Office monitored Fujitsu's PCI compliance closely using Weekly Highlight Reports for PCI compliance which tracked where Fujitsu were failing to meet their auditing or build requirements.[161][162]

154. Post Office also had a PCI Incident Response Plan in place from 18 February 2008, which set out key information relating to processes to be followed in managing defined PCI Incidents, including definitions of Minor and Major Incidents, roles and responsibilities at various stages of the Incident

---

142 This means compliance with the Payment Card Industry Data Security Standard ("PCI-DSS").
143 POL00398922
144 POL00398924
145 POL00399062
146 POL00399072
147 POL00393859
148 POL00393766
149 POL00399212
150 POL00397094
151 POL00397348
152 POL00397418
153 POL00397450
154 POL00401512
155 POL00397159
156 POL00397162
157 POL00397163
158 POL00397165
159 POL00397360
160 POL00324854
161 POL00396909
162 POL00396887

WITN03680200

management process, the method by which management would be informed of an incident, and reporting and testing requirements.[163]

b) The adoption of measures to rectify bugs, errors and defects within the Horizon IT system

PEAKs and KELs

155. I understand from a Terms of Reference document dated 30 July 2014, that Fujitsu convened a **Business Impact Forum,** as part of the Customer Service Improvement Plan, whose remit was to meet weekly to *"govern the assignment of PEAK Incidents".* I have detailed further below that I have been unable to establish Post Office's involvement with this Forum. PEAK was the incident and problem management system used by Fujitsu to log, diagnose and track the progress of reported Horizon incidents and problems from detection to resolution. Each incident/problem was assigned a PEAK number.[164]

156. It is my understanding that not all PEAKS would have been taken to or discussed at the BIF and it is not clear to me how Fujitsu determined which PEAKS, if any, merited escalation to the BIF.

157. On the basis of the information that I have reviewed for the purposes of this statement, it appears that for each PEAK being considered there should have been one of the following outcomes:

a. (i) **Approved** by the BIF, and the PEAK was to targeted in the next part of the meeting, being the Peak Targeting Forum. It is my understanding

[163] POL00397377
[164] POL00256092

WITN03680200

that this means it was accepted there was an error so that the PEAK could be added to the KEL;

b. (ii) **Request further information (from originator or other)** and defer to a subsequent BIF; or

c. (iii) **Add to the KEL** and close the Peak.

158. The processes appear to have been designed to consider a range of factors associated with the control and assignment of PEAKs, including, severity of the business impact, impacts of development, estimating, employment and costs of resolutions. It is my understanding that a PEAK would be considered either within the Business Impact Forum (if approved from a list of potential PEAKs to be considered), and separately the PEAK Targeting Forum would *"agree a target release for a PEAK*[165] *brought to the Forum".*[166]

159. The Terms of Reference document that I have referred to above appears to have been Fujitsu-generated, and although it includes the Post Office logo, I am unable tell from the document itself what Post Office's involvement in the BIF was. From a LinkedIn search that I have carried out as part of my preparation from this statement, I have been able to confirm that all the individuals listed amongst the membership and representation for the Business Impact Forum in this document were Fujitsu rather than Post Office employees. I also note that the document did not provide for any external circulation. I have made enquiries with members of the Post Office business who were in post at the relevant time to try and ascertain further information as to whether Post

[165] This would be the planned date of release when the PEAK fix would be applied to the live Horizon system.
[166] POL00400641

WITN03680200

Office was involved in this forum, and/or the degree of any such involvement with and/or Post Office's knowledge of the reporting from this forum, but unfortunately I have not been able to ascertain any further information which would enable me to assist the Inquiry further on this issue.

160. I have reviewed a set of Fujitsu PowerPoint slides dated (from an analysis of the metadata) 18 December 2015. These slides appear to refer to the role of the Business Impact Forum in the '*lifecycle of a defect*' and set out proposals for Post Office to become involved through a '**Joint Emergency Business Impact Forum**' which, it is stated, would be attended by Post Office Head of Service.

161. However, as has been the case with many documents in this statement, I have reviewed this document in isolation and have not seen any contemporaneous related documents As a result, I am not able to confirm when and to what extent the processes referred to in the slides were ultimately established, but a later operational spreadsheet that I have seen indicates that Post Office did authorise certain releases through a joint Business Impact Forum (the example I have seen is from 2019).[167]

2013 – 2019

(a) The identification, investigation, recording and reporting of (i) bugs, errors and defects in the Horizon IT system; (ii) other network and system failures or (iii) the impact of such events on branch accounts;

[167] POL00401529

WITN03680200

ATOS and the Tower Model

162. Fujitsu was, and remains, one of a number of IT contractors engaged by Post Office to facilitate various aspects of its business infrastructure. Other contractors, by way of example, included Accenture, IBM, Verizon, Computacenter (the "Supply Chain Members"). These contractual arrangements formed what was defined as the Post Office IT Supply Chain.

163. As was increasingly considered best practice across the public sector at the time, Post Office concluded by 2013 that management of the Supply Chain Members needed to be centralised and optimised, in order to facilitate better oversight of the maintenance and service associated with Post Office 's IT systems.

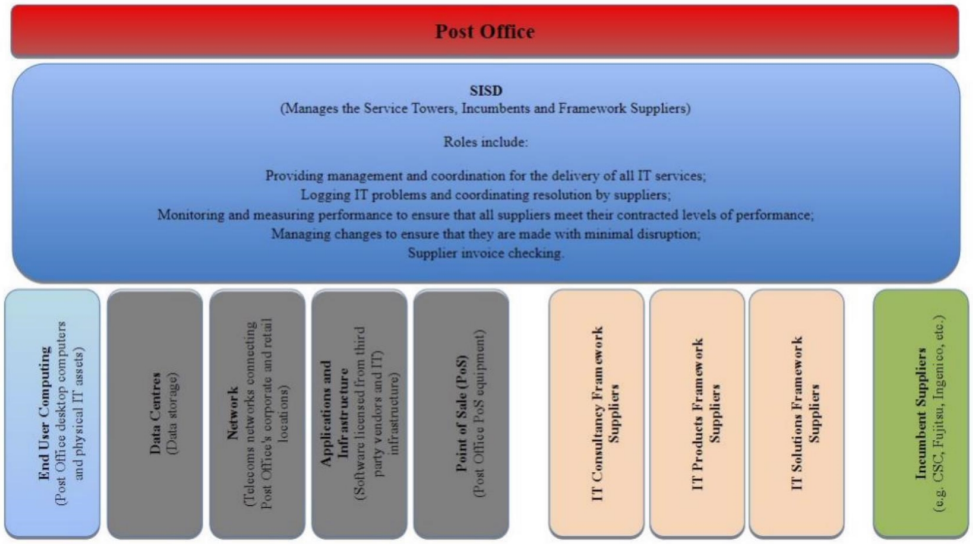
164. In 2013, following a successful procurement process, ATOS was appointed to manage the overall performance of a number of these Service Towers.

165. It is my understanding, based on discussions that I have had with colleagues who were in post between 2013-2019 (which I refer to further below) and from the document entitled "*Post Office IT&C Transformation Project Procurement Guide*"[168] that ATOS was responsible for managing incumbent suppliers of Post Office's IT systems, which included Fujitsu.

166. It is my understanding that ATOS's approach, on appointment, was to adopt **System Integration and Management (SIAM)** tools to track incidents, problems and the change process across the Supply Chain membership.[169]

[168] POL00398051, p.3
[169] POL00401616

WITN03680200



167. I have reviewed a document entitled, '*POL SISD governance Model: Terms of Reference'* dated 21 March 2014,[170] which illustrates how the working relationship between ATOS, Post Office and the Supply Chain Members was intended to be structured through a series of forums, each of which would have a focussed remit and report 'upwards'. The forums were categorised into the following levels: strategic, "S", management, "M", and operational, "O". The structure of these forums was, as I understand it, as follows:

[170] POL00398109

WITN03680200

Level	Committee / Forum / Meeting
Strategic	S1 – CIO Steering Committee
Strategic	S2 – Enterprise Architecture Committee
Strategic	S3 – Executive Relationship Forum (Part 1 & Part 2)
Management	M1 – CIO Management Committee
Management	M2 – IT Change Portfolio Committee
Management	M3 – Architecture Review Committee
Management	M4 – IT Supplier & Service Committee
Management	M5 – Information Security Management Forum (POL)
Management	M6 – Information Security Management Forum (SCM)
Management	M7 – Governance Review Committee
Management	M8 – Innovation Forum
Management	M9 – Information Assurance Management Forum
Management	M10 – Business Relationship Management Forum
Operational	PO1 – ITIL Performance & Service Review Committee
Operational	PO2 – IT Service Commercial Committee

168. The recollection of the colleagues that I have spoken to who were involved at an operational level with these arrangements between 2013 and 2019 was that the 'O', operational and 'M' management forums were all established and implemented through regular meetings with formalised reporting structures. However, in practice, the S1 (CIO Steering Committee), S2 (Enterprise Architecture Committee) and S3 (Executive Relationship Forum) were not formally stood up. The shared understanding and recollection from my colleagues was that instead, the topics that should have been discussed at the "S" level meetings were discussed at quarterly meetings at the executive level.

169. Having read the Terms of Reference for the SISD Governance Model, it appears that the operational meetings were low level meetings, the outputs of which were escalated to the management meetings (if required).

WITN03680200

170. Mandatory attendees at the '**M4 – IT supplier & Service Committee**'. from Post Office were: IT Change Lead, IT Procurement Lead, IT Governance and Controls, ISA Senior Compliance Manager, BRM Lead, and from ATOS: Service Delivery Director, Service Managers, and CTO.

171. The objectives of the **M4** forum included:

"a) Review effectiveness of the IT operation: - governance – services performance – services scorecard and policies b) SISD Programme Level Issue Resolution Level 3 Escalation – RUN/BAU Issues", and "Establishes and manage SLAs, Contractual Breaches to invoke penalties or incentive payment".[171]

172. The objectives also included a requirement to, *"Manage Commercial/contractual aspects of IT Suppliers (new and existing)"* and *"Manage top-level service risks and issues",* but for the reasons set out below, my understanding is that this would have applied to most Supply Chain Members but not to Fujitsu.

173. The M4 forum was supposed to meet monthly, for 1 day, and to consider in spreadsheet from:

"a) Supplier performance review (Operational Scorecard Summary with key KPIs – consolidated service performance exceptions and resolution plans b) Escalation from Issue Management Level 2: Escalated SISD Programme Level issues – RUN/BAU issues (SSID 4.0 Governance & Assurance)" and "The

[171] POL00398100, p.34

WITN03680200

detailed performance booklet of all the Incumbent SCM's SLAs/Scorecards (IT Service etc.)".[172]

174. M4 was tasked to produce, Minutes and a record of *"Issue Resolution or Further Escalations to Level 4 (CIO Management Committee)"*.[173]

175. The mandatory attendees at **M5 ISMF meetings** were, as I understand it, in so far as Post Office was concerned, the Information Security and Assurance Group **("ISAG")** Senior Technical Assurance Manager[174], and from ATOS: Security Operations Manager, Risk Manager, and SISD Quality Manager. Supply Chain Member representatives of Security Operations and Risk and Audit Compliance were optional attendees.[175]

176. It is my understanding that, during the period of the ATOS contract, Post Office would continue to attend ISMF meetings but that ATOS would chair the meetings and the associated reporting would be in the ATOS proposed format.

177. The structure illustrated in the SISD Terms of Reference document that I have referred to above was supported by a number of more detailed documents which set out the nature of ATOS's service provision.

178. By way of example, I have reviewed an ATOS prepared document entitled *'POL Security Management Plan [Draft]'* from July 2013'[176] which outlined how the provision of services by ATOS to Post Office would achieve an adequate

[172] POL00398100, p.34
[173] POL00398100, p.36
[174] It is my understanding that this would normally be a project role assuring the build standards being applied by technical development teams.
[175] POL00398100, p.39
[176] POL00399459

WITN03680200

level of security. That document contained a number of specific examples as to how that objective would be achieved in practice:

a. *'Information Security Incident and Weakness Reporting'*[177]Page 33, 8.9.1 – *'Accounting and Audit'*,[178]

b. Under 8.11 '*Fault Logging',*[179]

179. The development of ATOS's role in managing the service provided to Post Office by its Supply Chain Members is further demonstrated by the fact that, in 2012, Post Office produced its own IT & Change Weekly Highlights Report[180] whereas by 2013 'risks and issues logs'[181] were maintained and produced by ATOS.

180. In a later IT&C Transformation Programme Executive dashboard dated 14 December 2012, it was stated that Fujitsu had retrenched from the proposed obligations detailed in the Transitional Support Service contract to the obligations and timelines detailed in the Codified Agreement.[182] This appears to have delayed the implementation of *"milestones"* for the Tower model as defined by the IT&C Board at the start of 2013.[183]

---

[177] POL00401508, p.14. §4.2 *"Any suspected Information Security incident or weakness associated with the Post Office Ltd. Service which is identified/suspected by Atos staff will be reported to the contract Service Desk who will then follow the escalation procedures for the Incident and Problem Management, whilst ensuring reporting is escalated to both Atos, Post Office Ltd. And the Supply Chain, where appropriate."*

[178] POL00401508, p.33. §8.9.1 '*The Atos Post Office Ltd. Security Operations Manager will review physical and logical logs in order to meet service consumer requirements. Furthermore, as defined within Schedule 2.5, Atos will conduct compliance reviews across the Supply Chain where appropriate to ensure service levels are maintained.'*

[179] POL00401508. §8.11 *"The Atos Post Office Ltd. Service Manager will ensure that all faults are recorded in the Service Desk."*

[180] POL00397409; POL00397440; POL00397379.

[181] POL00399501

[182] POL00397903

[183] POL00397925

WITN03680200

181. By 2013, Post Office anticipated that the provision of the Horizon system by Fujitsu would soon be replaced by an alternative system which was to be provided by IBM. As a result, it is my understanding that the lack of agreement from Fujitsu in relation to the Tower model structure that I have described above was not assessed to be problematic at that stage.

182. It is my understanding that Fujitsu did report to ATOS in some respects, and ATOS was responsible for large parts of monitoring of Fujitsu's daily compliance with its contractual obligations (at a service level).

183. However, it is my understanding that the underlying responsibility for managing the Fujitsu's contract, monitoring Fujitsu's compliance with the relevant contractual obligations and assessing and taking forward any associated consequences in relation to the breach of those obligations remained with Post Office throughout the 2013-2019 period.

184. As a result, there was a separation between the management and monitoring of the service that was provided by Fujitsu pursuant to the Codified Agreement and the management and monitoring of services provided to Post Office by other IT suppliers.

ATOS monitoring and reporting in relation to the Horizon service as provided by Fujitsu

185. I have reviewed an ATOS *"POL Service Level Tracker",* which includes a consolidated table for Fujitsu's monthly service level performance throughout 2017, including SLAs for exception and error resolution.[184]

[184] POL00325396

WITN03680200

186. I have also reviewed a draft document titled *"Post Office SISD Contract Handbook"* which appears to indicate the different types of reports that ATOS was supposed to provide to the Post Office. These included reports in relation to performance management, such as monthly performance management reports, quarterly summaries, continuous maintenance schedules and periodic satisfaction surveys taken across the supply chain.[185]

187. It is my understanding that, in practice, during this period Fujitsu would attend meetings and provide agreed reporting to ATOS[186] but would not pursue actions in relation to their contractual obligations unless instructed by Post Office.

188. ATOS appears to have engaged, on a daily basis, with Fujitsu in respect of, among other things, reporting, SLA achievement, problem management and the Horizon service desk. ATOS regularly produced packages of data (for example, Service Review Reports,[187] an 'Atos Dashboard' and 'Atos Performance Summary',[188] Service Desk Risk Logs,[189] Service Level Trackers[190]). However, I have not been able to establish the extent to which Fujitsu's compliance with the relevant contractual obligations was captured within that reporting.

189. It is my understanding that there were no contractual provisions in place that required ATOS to carry out monitoring of Fujitsu's compliance with the relevant contractual obligations. It is my understanding that, during the period of the ATOS contract, the Fujitsu/ Post Office problem management processes (which

[185] POL00398086 (Version 2.0 January 2014), p.69
[186] POL00399522, 'Governance' tab
[187] POL00400226, POL00399592.
[188] POL00399751
[189] POL00399522
[190] POL00399525

WITN03680200

are set out at paragraphs 123-129 above and which were used to monitor the relevant contractual obligations in the period that pre-dated the Tower Model and ATOS's involvement) appear to have been maintained and updated where new functionality was introduced but otherwise came under the umbrella of the Current Contract. It therefore was, as I understand it, through those processes that Post Office monitored Fujitsu's compliance with relevant contractual obligations as defined in sections 2(a) and (b) during the period of the ATOS contract.

190. I have detailed below, based on a review of associated documentation from that period, how that process appears to have worked in practice.

191. In March 2013, a joint working document was prepared for review between Fujitsu and Post Office titled *'Operational Business Change – Branch Operational Level Agreement'* v.1.4.[191] This document appears to have referred to the interaction between Post Office and Fujitsu in the delivery of the OBC Branch Service for changes in branches[192]. It was a non-contractual agreement providing further clarification of the procedures used to deliver that service, and the measures that will be reviewed to assess its effectiveness.

192. In the same month, an interface agreement (CCD) was prepared and circulated for approval.[193] The purpose of the CCD was referred to as being to "*establish effective co-operation between Fujitsu Services and Post Office Ltd for the timely efficient and cost effective delivery of Operational Business*

[191] POL00397932
[192] The OBC process is a process used to make minor changes that would not require any amendment to the Codified Agreement. The opening of a new branch would be one such example of a minor change.
[193] POL00397971

WITN03680200

Change using Reference Data to HNG-X enabled Post Office counters".[194] The document was updated to reflect changes to the Reference Data Management Service and provided that Fujitsu would work jointly with Post Office to "*improve the quality and effectiveness of the Reference Data interface*"[195]. Pursuant to this agreement, Fujitsu were required to "*produce reports and send them to the relevant PO unit, and PO are to check reports and if errors are found submit a fresh change and should PO find an error during the 48 hour window a direct request to Fujitsu (usually by telephone) may be made to stop the release of the data. In this instance the release is no longer pre-authorised and becomes a change which requires authorisation*".[196]

193. The document also set out the process for processing errors, specifically outlining that all observed errors would be recorded as pre-live incidents.[197] There was also discussion within the document about processes for addressing Peaks and the "*agreed mechanisms for passing Peaks from the Fujitsu Services Peak system to Post Office Ltd and entering responses from Post Office Ltd into the Peak system*".[198]

194. I have also reviewed a document that was entitled *'Security Management Service Description'* dated 4 April 2014 which set out the approach to problem reporting and compliance in respect of Security Incidents.[199][200] In the sections

---

[194] POL00397971, p.19
[195] POL00397971, p.20
[196] POL00397971, p.28
[197] POL00397971, p.59
[198] POL00397971, p.64
[199] POL00393768
[200] A Security Incident is described in Post Office policy documents (e.g. POL00395097) as *"an adverse event or series of events that comprises the confidentiality, integrity or availability of RMGA information or information technology assets, having an adverse impact on Fujitsu Services' reputation, brand, performance or ability to meet its regulatory or legal obligations."* Such incidents could include a cyber-attack, the loss of a secure asset or a report of password sharing (at the lowest level).

WITN03680200

outlining the Security Management Services' focus on incident reporting and problem resolution,[201] it was *"agreed between POL and FJS these will be produced and made available to the Information Security Management Forum (ISMF) and Service Management Reviews (SMR)."*

195. It is my understanding that some important aspects of the HNG-X did not have Service Level Agreements and were developed and operated without reference to ATOS. An example of this in practice can be found in the September 2014 *'HNG-X Architecture – Security Architecture'* agreement between Post Office and Fujitsu.[202] This agreement created an automated event reporting mechanism that detected issues and created alerts and reports concerning network-wide patterns that could suggest a network error or failure to the Fujitsu account security team, which was known as the Security Event and Information Monitoring (**"SEIMS")** system. Any incidents would be escalated through the ISMF, and if necessary, the major incident process.

196. I have also reviewed a document entitled *'Description of Fujitsu's System of IT Infrastructure Services supporting Post Office Limited's POLSAP and NHG-X applications',* with iterations for the period April 2013 to December 2013[203] and April 2014 to December 2014[204] which describe particular mechanisms for reporting, auditing and incident management of those services, apparently without reference to ATOS.

197. In 2016, it is my understanding that the arrangements for Problem Management interfaces were formally revisited to take account of the role of

[201] POL00393768, p.12-14. §§2.1.8 – 2.1.12.4.
[202] POL00398421
[203] POL00235089
[204] POL00399609

WITN03680200

ATOS. A document entitled, *'Fujitsu Services / Post Office Limited Interface agreement for the Problem Management Interface',* dated 9 March 2016, set out "*the working relationship between Fujitsu Services and Post Office Limited for the Problem Management interface between ATOS, on behalf of Post Office, and Fujitsu Services Post Office Account [and defined] the interaction required between ATOS, on behalf of Post Office and Post Office Account when cross-domain problems are raised and reviewed.*"[205] The agreement set out the three parties' respective responsibilities as follows:

"5 Responsibilities

5.1 Joint

Each party is responsible for maintaining and updating their own problem databases.

When a new cross-domain problem is identified in either domain the party who identified the problem is to submit a new Problem Record Template (See Appendix 1) to the other party, thereby ensuring a consistent problem record exists in both domains.

Both parties will maintain a shared cross-domain Problem Management spreadsheet which is independently updated on a weekly basis by both parties and reviewed on a weekly basis at a cross-domain Problem Management review. This spreadsheet is to detail the problem record reference for both domains.

Each party will nominate a problem manager for all cross-domain problems.

[205] POL00401517

WITN03680200

Each party will ensure their counterpart problem manager is appraised as appropriate of the current situation/status of the problems. Both parties will authorise Temporary Procedures/Authorised Temporary Procedures impacting on the Post Office operating process for cross-domain problems. Both parties will provide incident reference(s) from their respective service desk calls to the associated cross-domain problems. Each party will ensure their counterpart problem manager is notified if problem ownership changes (i.e. if ownership changes from one FJ POA problem manager to another the original problem manager must notify their counterpart problem manager and vice versa).

5.2 ATOS Specific Responsibilities.

ATOS Problem Management will own the weekly problem report spreadsheet, which should detail all 'open' problems, including those that it has been jointly agreed should be on 'monitoring'. POL will manage aspects of any problem relating to the operating process within the Post Office front line e.g., office process & back end systems e.g. CFS, etc. POL own management of any planned communication with the branches, e.g., Message Broadcast Service.

5.3 Fujitsu POA Specific Responsibilities

Fujitsu Services POA will update and maintain individual problem records in their Problem Management Database. Fujitsu Services POA will manage any problems technical and physical originating in the Fujitsu domain. Fujitsu Services POA will undertake an annual review of problem records from the perspective of identifying from those records any trends for which underlying

WITN03680200

cause corrective actions could be implemented. E.g., Process improvements, additional test methodologies, etc."[206]

(b) The adoption of measures to rectify bugs, errors and defects in the Horizon IT system

198. It is my understanding that the arrangements and measures that were put in place to rectify BEDs in the Horizon system that I detailed above in paragraphs 155-161 continued until 2016 when the *'Fujitsu Services/Post Office Limited Interface agreement for the Problem Management Interface'* that I have referred to above was introduced.

199. The Interface explained the processes for remedying problems in the Horizon IT system which continued to involve the investigation of a problem's root cause (including through the introduction of temporary procedures as necessary[207]) and the application of an effective solution.

200. Whereas problem management had previously been primarily the responsibility of an appointed Fujitsu Problem Manager (see paragraphs 123-129), under the Interface ATOS Problem Management and Fujitsu would manage problems collaboratively and (as noted above in paragraph 192) both parties would appoint problem managers in relation to cross-domain problems which would include BEDs and other system problems. The Interface document summarises the problem management responsibilities held by ATOS Problem

[206] POL00401517, p.9.
[207] POL00393885. Temporary procedures could be used as an interim solution for a problem until such time as a permanent solution to the problem was established.

WITN03680200

Management and Fujitsu in relation to the investigation of problems, information sharing. agreement to temporary procedures and problem closure, as follows:

a. *"Management of any cross-domain problem will include the following stages:*

b. *Analysis (to determine root cause)*

c. *Control (TP or ATP implementation, escalation)*

d. *Resolution (review and closure)*

e. *Analysis –*

f. *The relevant domain (which would be the party that was required to carry out the analysis, whether that was Fujitsu, a third-party domain[208] or ATOS) will carry out the analysis to determine the extent and impact of any specific problem. It may also mean the implementation of "traps" to pick up any further occurrences before the root cause can be established. Once the root cause has been established, a description and date identified will be disseminated to the other business as an effective measure of the Problem Management process. As the analysis progresses initial perceived root causes may change.*

g. *Incident Matching - Both domains will exchange volumes of incidents to associated problems to an agreed timescale which would normally be on a weekly basis (dependant on the problem).*

h. *Control – This covers escalation of problems as necessary and the introduction of Temporary Procedures (TP - exclusive to each domain but does not impact the other domain in conducting it's business as*

[208] It is my understanding that this definition could relate to a technical domain used to provide services.

WITN03680200

usual) or Authorised Temporary Procedures (ATP - Agreed between each party). Audit trails will also be maintained within each domain that enable tracking of actions or interaction between the two domains.

i. *Resolution – Cross domain problems can only be closed when both domains agree that the closure criterion has been met without compromising any other services. Both domains will provide a review of all problems to determine if the solution provided has actually removed the problem. Closure may be after a monitoring period and will be agreed by both parties."*[209]

201. The document made detailed provision for associated processes, such as a **Problem Management Operation Review Forum**, and a Post Problem Implementation Review Meeting. There were provisions for escalation that required ATOS ultimately to escalate to an ATOS senior manager a problem in their domain, and Fujitsu to escalate directly to Post Office.

The 'Horizons Issues Working Group'

202. Separately from these processes, a '**Horizon Issues Working Group**' held a call between July 2013 to around March 2019 and met broadly weekly initially and fortnightly after 2014. From October 2013, the call came within the remit of the Branch Training and Support Programme. The purpose of this Working Group was to identify and discuss issues which might impact on or be impacted by the points raised in Second Sight's interim report.[210] It was set up so that the

[209] POL00401517, p.11
[210] POL00137533

WITN03680200

right people across the Post Office business had the appropriate level of visibility to ensure a consistent approach was adopted to managing issues raised with Horizon. Minutes show specific complaints from branches and other sources were discussed, and their escalation and resolution tracked.

Monitoring by the Strategic Group Executive and the POL Board

Risk and Compliance Committee

203. Post Office's **Risk and Compliance Committee** was, until 2012, a Board Level Committee. However, from 2012 onwards, it was a Strategic Group Executive (SEG or GE) level Committee. The references below to the Committee relate to the period from 2012 onwards.

204. It appears that one of the purposes of Post Office's Risk and Compliance Committee (in addition to monitoring Post Office's PCI compliance (and wider compliance with industry standards) [211]), was also to monitor any contractual non-compliance by members of the Post Office Supply Chain (including Fujitsu), enforce compliance[212] and track any associated work undertaken by the contracting party .[213] [214] [215] [216] It is my understanding that formal internal reports were occasionally produced [217][218] For example, ATOS were criticised in a June 2016 Chief Information Officer **("CIO")** Risk and Issues Log for failing to understand and implement POL[OBJ][219]

[211] POL00397399
[212] POL00401627
[213] POL00401626
[214] POL00401628
[215] POL00401629
[216] POL00400766
[217] POL00401626
[218] POL00401625
[219] POL00400133

WITN03680200

205. I have reviewed the minutes of a meeting of the **Risk and Compliance Committee** which took place on 28 September 2016.[220] This was attended by (among others) CEO Paula Vennells, CFO Alisdair Cameron, GC Jane MacLeod, and representatives from Ernst & Young. The Committee discussed a Horizon outage that had occurred on 9 May 2016 and the '*lessons learned*' from that, incident, including what changes were required to be made to IT systems and incident management process. It was stated "*clear information flow and joint working has been established with ATOS*".[221]

206. The document suggests that by May 2017 Post Office was acknowledging there were some difficulties in the arrangement with ATOS. The minutes of a Risk and Compliance Committee meeting on 4 May 2017[222]suggest that the committee was informed that, "Problems are actioned and then closed by Atos without PO's knowledge or briefing. Once a call is logged there is no visibility for PO as to how it is dealt with. The problem management process needs to be further improved as Atos do not review problems from suppliers out with their tower arrangement."

207. It is my understanding from the conversations with colleagues who were in post between 2013-2019 that it eventually became clear that there was a list of services that ATOS was not able to fulfil pursuant to the Tower Model. This was because ATOS consistently failed to deliver a sustainable service, improve technology, manage the IT Supply Chain or add value across the service lines by communicating effectively and performing effective root cause analysis.[223]

---

[220] POL00400101
[221] POL00400101, p.132
[222] POL00401624, p.46 'Item 3'
[223] POL00401616

WITN03680200

208. As a result, Post Office incrementally began to end the services being delivered pursuant to the ATOS contract and conducted a staged exit from that contract between 2018 and 2020.

209. A document dated July 2018 indicates how Post Office analysed its position at the time:[224]

"3. Lack of formal systems integrator and SLA monitoring Finding …

The Branch Technology project[225] is heavily reliant on third party vendors, to deliver the project. POL are following the Government's Towers Operating Model to deliver the project. Computacenter are responsible for the hardware base build and coordinating the installation of the terminals, via a further third party (ByBox). Fujitsu have been responsible for the development of the application and Atos are responsible for first line support. However, the review identified:

a. *There is no longer a systems integrator to coordinate the activities of the third parties to support successful delivery. Project Team members have tried to fill this role by meeting with vendors on a regular basis to fix urgent issues. However, these activities are not centrally coordinated and the outcomes of the meetings are not shared across the entirety of the third party eco-system.*

b. *We were informed that POL have not been able to alternatively contract without additional risk and cost, however this decision has not been documented.*

---

[224] POL00400632

[225] POL00400397 describes the Branch Technology Project as starting in 2015 and being "*...initially scheduled to deliver 22.500 counter terminals by June 2018 at a total cost of £49m*" I understand, from this document, that costs increased by 9% as a result of an incorrect estimate of the number of terminals required and associated licensing costs.

WITN03680200

c. *We acknowledge that difficulties have been experienced with Computacenter's delivery of the project and contract managers receive high level performance information but this is not detailed information that is aligned to SLAs.*

d. *As a result, monitoring of SLA performance is not performed by the project (due to lack of SLA knowledge) or by contract managers (due to lack of detailed information). The contract managers are also not part of the project management team.*

e. *Risk."*

There is a risk that POL pay for services that are not delivered or contractual requirements are not fulfilled."[226]

210. ATOS's role in the service management of or reporting in respect of Fujitsu was one of the first services that was stopped.

[226] POL00400632, p.5

WITN03680200

Level	Committee / Forum / Meeting
Strategic	S1 – CIO Steering Committee
Strategic	S2 – Enterprise Architecture Committee
Strategic	S3 – Executive Relationship Forum (Part 1 & Part 2)
Management	M1 – CIO Management Committee
Management	M2 – IT Change Portfolio Committee
Management	M3 – Architecture Review Committee
Management	M4 – IT Supplier & Service Committee
Management	M5 – Information Security Management Forum (POL)
Management	M6 – Information Security Management Forum (SCM)
Management	M7 – Governance Review Committee
Management	M8 – Innovation Forum
Management	M9 – Information Assurance Management Forum
Management	M10 – Business Relationship Management Forum
Operational	PO1 – ITIL Performance & Service Review Committee
Operational	PO2 – IT Service Commercial Committee

211. The structure illustrated in the SISD Terms of Reference document that I have referred to above at paragraph 165 was supported by a number of more detailed documents which set out the nature of ATOS's service provision.

212. Whilst Post Office was able to structure its contracts with most of its Supply Chain Members to facilitate each of them reporting to and engaging with ATOS under the Tower scheme that I have described above, Fujitsu did not agree to amend the terms of the Current Contract to facilitate it engaging with ATOS in the same way. I have reviewed an IT and Change ("**IT&C**") Programme Transformation Programme Board Update from 16 April 2012 which refers to the fact that a low level of engagement from Fujitsu was causing issues to the

WITN03680200

successful management of the procurement process for the IT&C Transformation programme.[227]

213. However, when it subsequently transpired that the Horizon system would not be replaced by an IBM product, it was necessary to instead extend Fujitsu's provision of Horizon. The consequence of this was that Fujitsu's delivery of the Horizon system did not sit effectively within the Tower Model.

214. As a result, there was a separation between the management and monitoring of the service that was provided by Fujitsu pursuant to the Codified Agreement and the management and monitoring of services provided to Post Office by other IT suppliers.

215. ATOS appears to have engaged, on a daily basis, with Fujitsu in respect of, among other things, reporting, SLA achievement, problem management and the Horizon service desk. ATOS regularly produced packages of data (for example, Service Review Reports,[228] an 'Atos Dashboard' and 'Atos Performance Summary',[229] Service Desk Risk Logs,[230] Service Level Trackers[231]). However, I have not been able to establish the extent to which Fujitsu's compliance with the relevant contractual obligations was captured within that reporting.

[227] POL00397400
[228] POL00400226; POL00399592.
[229] POL00399751
[230] POL00399522
[231] POL00399525

WITN03680200

216. ATOS's role in the service management of or reporting in respect of Fujitsu was one of the first services that was stopped.

Contractual updates relating to Post Office's internal monitoring of Fujitsu's compliance with the relevant contractual obligations as defined in sections 2(a) and (b)

217. On 3 July 2017, schedules of updates to the **Current Contract** recorded the agreed process for recording whether Fujitsu was fulfilling its delivery obligations in respect of Project HNG-X.[232] It included a mechanism for managing '*rectification activities*' that were required to fulfil any Acceptance Criteria that Fujitsu had not met. It described the *'incident severity matrix'* which was, as I understand it, used to categorise incidents based on their severity and impact on the HNG-X Acceptance Process.[233]

218. To summarise, these were:

a. **High Severity:** Incidents that result from HNG-X or associated changes causing defects which rendered critical elements of Business Capabilities, Support Facilities, or Infrastructure unfit for operational use. Examples include preventing transactions, hindering business inputs or outcomes, or causing performance issues that breach service level targets.

[232] POL00393769
[233] POL00393769, p.22, Annex A

WITN03680200

b. **Medium Severity:** Incidents resulting from HNG-X changes causing defects that do not stop operations but create problems in using certain transaction types.

c. **Low Severity:** Incidents caused by HNG-X changes resulting in defects without any adverse operational impact or those that can be resolved by Fujitsu Services without affecting Post Office operations.

d. **Non-Incident:** Cases investigated and no defects, unrelated to HNG-X changes, or not part of the HNG-X Acceptance Process.

219. Annex C of the document described a number of '*acceptance methods*' through which Post Office could satisfy itself that Fujitsu had met the service levels required of it pursuant to the Current Contract.[234]

220. It is my understanding that HNG-X Acceptance the status of an incident. If they could not agree then the incident would be escalated to the HNG-X Acceptance Dispute Board for resolution. In the event that an HNG-X Acceptance Dispute cannot be resolved by the Dispute Board, it would be escalated for Executive Review and dealt with in accordance with the Dispute Acceptance Procedure.[235]

Senior/Board monitoring of Fujitsu's contractual compliance (whether through direct oversight or receiving reporting).

221. I have not been able to establish a clear picture of the extent to which the Post Office Board, the Board sub-committees, the Strategic Executive Group

[234] POL00393769, p.24, Annex C
[235] POL00325152

WITN03680200

(formerly Group Executive) and its sub-committees were involved in the monitoring of Fujitsu's compliance with the relevant contractual obligations as defined in sections 2(a)-(b).

222. From the documents that I have reviewed, it does appear that there was some monitoring at those senior levels.

223. To the limited extent I have been able to establish it (and locate associated documents) I have detailed this further below.

POL Fujitsu Executive Steering Board

224. It is my understanding that the Post Office / Fujitsu Executive Steering Board appears to have met between January 2014[236] and September 2016[237] with the purposes of acting as the primary technology leadership group and the most senior open[238] forum in Post Office's technological infrastructure.

225. It is my understanding, based on the limited associated information and documentation that has been able to be located for that period, that the purpose of the Board was to bring the technological leadership teams from the two organisations (Post Office and Fujitsu) together, act as a point of escalation for disputes and to oversee financial and service performance.[239]

226. It is my understanding that, for the meetings held by this Board, PowerPoints were produced which included analyses of: Fujitsu's performance against service levels (such as those relating to branch network services and data

[236] POL00398082
[237] POL00400086
[238] I have not been able to establish what "open" means in this context despite making internal enquiries within Post Office.
[239] POL00398082

WITN03680200

centre operations);[240] the identified risks within the contractual relationship; contractual compliance;[241] and current service descriptions.[242]

227. It is also my understanding that the group commissioned external reviews and considered the extent to which actions needed to be taken pursuant to the findings of those reviews. [243] It is also my understanding that the group specifically discussed ways in which BEDs and NSFs may arise, for example, as a result of inefficient capacity testing.[244] The group appears to have recommended actions and assigned owners to specific risks that specifically related to the relevant contractual obligations within sections 2(a) and (b) of the Rule 9 request, such as functional issues caused by legacy operating systems.[245]

Reporting to the Post Office Board

228. I have reviewed the Minutes of a Board Meeting which took place in January 2015, with a pack of papers for a Board Meeting that was scheduled to occur on 25 March 2015.[246]

229. In those Minutes, it is recorded that an update was provided to the Board by the Audit, Risk and Compliance Committee ("**ARC**"). Minutes of meetings of the ARC were also included in the papers provided to the Post Office Board.[247]

---

[240] POL00398561
[241] POL00400086
[242] POL00400086
[243] POL00398561
[244] POL00400086
[245] POL00400076
[246] POL00353031
[247] See page 75 of POL00353031

WITN03680200

230. I have also reviewed a set of Post Office Board Minutes from a meeting that took place on 25 July 2016[248]. In those minutes, reference is made to the Chairman of the ARC updating the Board in relation to IT Security and a Horizon outage. It is my understanding, from those Minutes, that the Board requested a further strategy update in January 2017. However, as has been the case with other documents in this statement, I have reviewed this set of minutes in isolation and, as a result, have not been able to ascertain whether that update was ultimately provided to the Board.

231. I have also reviewed a set of papers that were provided to the Post Office Board by the ARC on 28 November 2016. In the section of those papers that was titled "Governance and compliance" reference was made to the following:

a. Risk and governance structures are in place and being embedded.

b. The most significant risk issue remains the operational oversight by Post Office of its branches.

Further examples of matters being escalated to Post Office's Senior Leadership

232. I have reviewed examples of Service Performance slide packs that were prepared by Post Office's then Head of IT Andrew Garner produced Service Performance Slide packs[249] between June and September 2016. These were sent to some members of Post Office's Senior Leadership Team. For example:

a. The March 2016 slide pack was sent to Rob Houghton[250] in an email dated 21 June 2016 and to Kevin Gililand, Angela Van-Den-Bogerd,

[248] POL00399587
[249] POL00242846
[250] POL00400007

WITN03680200

Nick Beal and Owen Woodley and others in an email dated 22 June 2016.[251]

b. The June 2016 slide pack was sent to Kevin Gililand, Rob Houghton, Nick Beal, Owen Woodley, Angela Van-Den-Bogerd, and others in an email dated 20 July 2016.[252] Some of the slides were included in a wider presentation at a CIO Operations Board Meeting at which Rob Houghton, Joe Arakji and others also delivered sections on 25 July 2016.[253]

c. The September 2016 slide pack was sent to Kevin Gililand, Angela Van-Den-Bogerd, Nick Beal, Owen Woodley and others in an email dated 19 August 2016.[254]

233. These slide packs analysed individual high severity incidents and tracked[255] them against the service levels expected of Fujitsu by answering the questions *'what happened to service performance?', 'what was done to improve it?',* and *'what is service performance doing now?'*. They aimed to evaluate whether the incidents were caused by known errors, propose ways that service management could be improved based on the findings of investigations into specific incidents, and continually track the number of incidents of different severities. Importantly, they ostensibly considered whether Fujitsu's performance of these service levels represented breaches of their contractual obligations.

[251] POL00242845
[252] POL00400037
[253] POL00401507
[254] POL00400116
[255] POL00401507

WITN03680200

234. It is my understanding that Risk Logs were also produced internally within Post Office for review and consideration by Post Office's CIO.[256] These Risk Logs included dashboards which categorised, quantified, and analysed identified IT risks and issues. These logs also included details in relation to each individual identified risk and its severity. For example, in a log from June 2016, the potential ineffectiveness of the failover system and the associated degradation of the Horizon system, which was leading to instability and increased failure rates, were flagged.[257]

External Monitoring of the extent to which Fujitsu was complying with the relevant contractual obligations within sections 2(a) and (b) of the Rule 9 request.

235. It is my understanding that, during the period that is the subject of question 3(b)-(d) of the Rule 9 request, Post Office would periodically commission external reports which appear to have reported on (amongst other matters) the extent to which Fujitsu was complying with the relevant contractual obligations.

236. A key example of such external engagement and associated reporting was the annual commissioning of an audit[258] by Ernst and Young to ensure that the Horizon system maintained its PCI Accreditation in relation to: ISAE 3402 – which details the standards for control measures like monitoring, risk assessment, performance management, system integrity and the governance of these activities. I have referred to these audit reports and the limited understanding that I have been able to establish regarding the associated

[256] Chief Information Security Officer
[257] POL00400133
[258] POL00398199

WITN03680200

actions taken internally within Post Office as a result below (see paragraphs 299-364).

237. I also understand that bi-annual reviews were scheduled to ensure that security controls consistent with the International Standard ISO27001:2005 Code of Practice (formerly BS7799) for Information Security Management were deployed for the Post Office Card Account[259] (POca) system.[260] [261] However, the reports were also intended to identify measures that would maximise customer experience and service level adherence. In 2013, Post Office commissioned Infosec to conduct this review. Infosec produced a risk action and treatment plan which was intended to be a living document that tracked actions against risks, provided details of compensating controls, and included confirmation of acceptance of risk or mitigation and closure.

238. I have not been able to identify any documentation that refers to what, if any, action was taken within Post Office as a result of this review.

REMOTE ACCESS RIGHTS

Question 2(c), 3(a) and 3(b): Regarding, "*the use of access rights and privileges by Fujitsu employees to remedy errors in transaction data and branch accounts*" (definition 2(c)), address, "*the Post Office's position on the nature and extent of the relevant contractual duties and how they changed over time*"

---

[259] These accounts were basic bank accounts for DWP to pay government benefit payments into.
[260] The Post Office Card Account Management service including, but not limited to:
Interconnection to the Branch Network via the Horizon System
Interconnection with the POca Banking System.
The document scanning and image storage service.
The document management system and its fulfilment centre.
The Customer Management System.
Post Office Limited POca control team for management information
The Secure Electronic Online Communications System (SEOCS)
The Bank of Ireland ATM Network.
[261] POL00393731

WITN03680200

(3(a)) and "*What, if any, internal or external measures were put in place to monitor Fujitsu's compliance with the relevant contractual obligations*" (3(b))

239. There is in any large commercial IT system a requirement for provision to be made for some technical users to have privileged access to databases. This is necessary in order for those users to carry out system maintenance and problem solving. The Horizon system included such facilities. The exercise of those access rights carried obligations intended to maintain the security and auditability of the system. Provision was therefore made that such access was only to be afforded to qualified and specified individuals, that supervision was in place when it was being exercised, and that it was auditable. I describe the relevant provisions for the existence of that capability and the processes surrounding it (see paragraphs 244-292), and for the requirements of supervision and auditing. In doing so, I describe both the contractual obligations set out in the Codified Agreements and CCDs and some of the relevant processes and expectations set out in Design Documents. I then separately set out the structures that were in place for Post Office to receive the regular reports that Fujitsu was required to make pursuant to these provisions (see paragraphs 292-297).

240. Having reviewed this material, it is my understanding that Fujitsu were required to monitor, document and report on their own exercise of access rights to the extent that Post Office were dependent on Fujitsu's assurances of its system's inbuilt integrity controls and auditability. It does not appear that there was any mechanism for Post Office itself to independently assess the accuracy of Fujitsu's reporting about its compliance with these obligations.

WITN03680200

241. Following my review of these provisions I summarise the external reviews that Post Office commissioned by way of periodic monitoring and review of Fujitsu's access rights, often as part of a wider audit of the integrity and security of Post Office's IT systems (see paragraphs 298-364). Where relevant, I summarise the formal steps that it appears Post Office took by way of internal response to concerns raised about access rights within those reports.

242. I understand that the facts and opinions expressed in this part of my statement will be of relevance to Phase 5 of the Inquiry and raise questions about historic public representations that Post Office has made about privileges and access rights, and about the stance that Post Office took about this during the GLO. I make clear that I have confined my statement on these issues to the questions posed in R9(48) and I do not attempt to anticipate or respond to any such questions in this document.

Processes in Codified Agreements and CCDs for remedying errors in transaction data and branch accounts

243. The contractual provisions that provided the outline obligations for affording the accesses required to enable remote remedying of errors in transaction data and branch accounts working within the Horizon System are set out below from paragraph 245.

244. I would note that whilst the question I am asked is about the remedying of errors in *"transaction data and branch accounts*" I have included in my review contractual provisions and documents that relate to the power to alter *'data'*, even where it may be that the text refers to *'data'* generally, and therefore may relate to broader category than specifically *'transaction data'* or *'branch*

WITN03680200

accounts'. That is because, particularly in respect of CCDs, policy, manuals and service descriptions, the documents have tended to describe facets of Horizon and its interfacing systems often do not distinguish between specific sub-categories of data within that system. As a result, where documents include references to forms of remote access to data or the correcting of data, it is not always clear to the reader whether or not those references are inclusive of transaction data specifically or are referring to that relevant part of the Horizon system. I also understand that the Inquiry is interested in whether access rights to data may have been misused, or used more widely than intended. I have therefore taken an inclusive approach rather than run the risk of erroneously excluding relevant provisions.

Codified Agreement

245. Original Codified Agreement

a. **Schedule A15 Clause 3.3.4.3** stated that the Transaction Management Service (**"TMS[262]"**) shall provide links into client systems operated on behalf of clients as required to support POCL.

b. *Schedule A2 Clause 4.16* stated that "*The confidentiality, integrity, availability, and completeness of data shall be maintained throughout all storage, processes, and transmissions, including during periods of Service Failure and recovery from Service Failure.*"

c. Schedule A16 Reference Number 812 stated that:

[262] Whose role was to provide a secure and resilient messaging and journalling service which shall support the transfer of data between OPS and Post Office Client Services, and Post Office Services

WITN03680200

i. EPOSS[263] will allow customer transactions to be reversed. EPOSS will also implement a mechanism to allow corrections to stock and cash transfers within the Outlet or between the Outlet and a remote location.

ii. EPOSS will allow reversals to transactions providing that POCL and Client accounting and business rules allow them.

iii. EPOSS will allow "*accounting adjustments*" in the form of correction transactions which are not necessarily mapped to specific transactions in the journal.

d. **Schedule A16 Reference Number 827** stated that the Pathway solution could support links to external computer systems. Such links were already in existence and were achieved through the use of a service specific TMS agent.[264]

e. **Schedule A16 Reference Number 800** detailed one of the processes for remedying an erroneous transaction. It stated that corrections to a transaction within the current customer session would normally involve a simple modification applied directly to the transaction, in which the original transaction would be reversed and the correct transaction would be inserted.

f. **Schedule A16 Reference Number 804** stated that that '*a loss or gain transaction may need to be generated to account for any cash (or other*

[263] Electronic Point of Sale Services
[264] means part of the Infrastructure that accesses TMS held data

WITN03680200

MoP[265]) *involved in the transaction*' when a user was browsing the transaction journal.

g. **Schedule G01 Clause 1.16.2.** stated that TMS shall provide links into other computer systems as required to support the introduction of new or reengineered Transactions required by POCL.

h. **Schedule G01 Clause 4.2.1.1.** stated that each instance of OPS[266] within outlets shall interface with TMS to allow the transfer, in both directions, of authorised data files and messages.

246. **2002 Agreement**

a. **Schedule 2 Clause 4.1.5,** "*The confidentiality, integrity, availability, and completeness of data shall be maintained throughout all storage, processes, and transmissions, including during periods of Service Failure and recovery from Service Failure.*"

b. **Schedule 18 Clause 7.3.3.3** stated that the Central Infrastructure and Telecommunications Infrastructure shall provide links into other computer systems as required to support the introduction of new or re-engineered Transactions required by Post Office.

c. **Schedule 18 Clause 2.6.2.3** stated that the Reconciliation Facility[267] receives data from the NBS Application[268] and from the Network Banking Engine **("NBE")** and prepares reports reconciling these data streams.

---

[265] This means a Method of Payment for e.g. DC MoP is a method of payment where the form of payment is a DC Token.
[266] OPS means the office platform service described in (as applicable) paragraph 4 of Schedule B4.3 or paragraph 2 in Part 1 of Annex 2 to Schedule B5.
[267] means the Applications referred to in paragraph 2.9 of Schedule 18.
[268] The application which supports transaction of banking business in Branches. It is installed at all Counter Positions in all Branches, but requires an operational data communications link in order to process Transactions.

WITN03680200

These were used to identify reconciliation exceptions for investigation and corrective action.

d. **Schedule 18 Clause 2.9.1** stated that the Reconciliation facilities are composed of various tools that reconcile the data generated between itself, its clients and third parties. These facilities will also support the reconciliation of accounting transaction data processed at a Counter Position with the details passed to the Post Office and details contained in the Branches Cash Accounts.

247. **Current Contract – Version 1 (2006)**

a. **Schedule A4 Legislation, Policies and Standards** stated, in Clause 4.1.5: "*The confidentiality, integrity, availability, and completeness of data shall be maintained throughout all storage, processes, and transmissions, including during periods of Service Failure and recovery from Service Failure*."

b. *Schedule B3.2 Clause 10.1.12* stated that the purpose of the Reconciliation Service was to provide end-to-end reconciliation and incident management procedures required to investigate, report and resolve reconciliation and business incidents.

c. *Schedule B3.4 Clause 64.4.3 and Schedule B4.4 Clause 62.3.3* stated that the HNG-X Central Infrastructure and HNG-X Telecommunications Infrastructure shall provide links into other computer systems as required to support the introduction of new or re-engineered Transactions required by Post Office.

WITN03680200

248. **Current Contract – Version 11 (2016)**

a. **Schedule B3.4 Clause 58.4.3** and **Schedule B4.4 Clause 134.3.3.3** stated that the HNG-X Central Infrastructure and HNG-X Telecommunications Infrastructure shall provide links into other computer systems as required to support the introduction of new or re-engineered Transactions required by Post Office.

b. **Schedule B4.2 Clause 121.9.1** stated that the Horizon Reconciliation Facilities comprise a set of applications which will support Post Office in effecting reconciliation between itself, its clients and third parties. These facilities will also support the reconciliation of accounting transaction data processed at a Counter Position with the details passed to the Post Office.

c. **Schedule B4.4 Clause 134.4.5.2** stated that the interfaces between the Data Centres and Post Office or Client systems shall support real and delayed time initiation of activities.

249. Further and more detailed provision for the capability and perceived need for privileged access for the remedying of errors in transaction data and branch accounts was made through CCDs, policy and design documents, which I have detailed below.

250. By way of example, the *'Access Control Policy'* stated that remedial action would be required as part of the monitoring of the system by Security Management and Operational Management, and that '*human*' intervention would only be required in "*exceptional circumstances*" and usually as a

WITN03680200

response to Incidents.[269] For example, SSC would generate flat files of transaction adjustments that would then be transmitted into data centres. Version 4 of the document, issued in July 2002, stated that auditors may also require access.[270]

251. The *'Reconciliation Service: Service Description'* explained that Fujitsu would provide a 'Reconciliation Service' to ensure financial integrity access all transactions in HNG-X.[271] It provided for a mechanism in which the Reconciliation Service would raise a 'BIM Report' (Business Incident Management Report). The BIM Report was to contain the details of the repaired transaction file or files (if a single BIM required multiple amendments)[272.] When making these changes, the Reconciliation Service were permitted to make corrective assumptions concerning the data based on previous patterns or types of data and communicated to Post Office.[273] [274] However, from December 2013 onwards, Version 4 of the document stipulated that the Reconciliation Service was required to seek permission from Post Office before inserting corrective transactions to address inconsistent records.[275]

252. There is a difference between **Version 1** of the document dated 24 August 2006 and **Version 4** of the document dated 3 December 2013.

253. Version 1 which provides at §2.1.4.17:

"*If the Reconciliation Service identifies that any Transaction data held on the 'central database' located at the. Data Centra is found to be inconsistent*

[269] POL00400810, v.1.0 dated 17 April 1997.
[270] POL00400776
[271] POL00394858
[272] POL00393950
[273] POL00394858
[274] POL00394858
[275] POL00400387

WITN03680200

when compared to the records of the Transaction that was completed at the Branch, e.g. a receipt, a Transaction log or a Branch accounting discrepancy, the Reconciliation Service shall obtain authorisation from Post Office prior to amending the centrally held Transaction data"[276] (emphasis added)

254. Whereas, Version 4 provides at §2.1.4.16 the same provision but the last sentence instead reads, "*… prior to the insertion of corrective transactions.*" (emphases added). [277]

255. This process was discontinued on 3 June 2020.[278]

256. The '**HNG-X Architecture – Security Architecture'** CCD was in place throughout HNG-X's rollout, from Version 2 released on 8 January 2009[279] to Version 4 released on 24 September 2020.[280] This is summarised again below in respect of how access rights were exercised, but it provided that there would be a connection between the Fujitsu Corporate network and the Horizon-Online infrastructure which would be used for "*support and reporting purposes.*"

257. The **'Customer Services Support Services Manual'** issued on 7 November 2000 stated that there were only two reasons for accessing the live system which were:[281]

a. Assisting in diagnosis of problems on the live system; and

b. Correcting data which has become corrupted subject to an Operational Correction Request which was required for this action.

[276] POL00394858, p.13
[277] POL00400387, p. 12
[278] POL00401578
[279] POL00397112
[280] POL00400323
[281] POL00400840

WITN03680200

258. The **'Operations Manual for the Customer Services Directorate,'** which was released on 24 August 2006, provided that access to the live system to correct data would only be permitted when data had become corrupted and only if an Operational Correction Request was submitted.[282][283] These were Fujitsu generated documents circulated to Post Office apparently for information only.

259. **Version 2** of the Policy, released on 24 February 1998, stated that individuals' roles had specific permissions associated with them. This was known as *'Role Based Access.'*[284] The system was intended to perform a check on whether the action an individual was attempting was compatible with their permissions.[285] It was intended that only some individuals had permission to use the tools that could impact branch accounts such as Tivoli and Oracle.[286]

260. Role Based Access also extended into which areas of the system an individual could access. For example, Post Office Systems and Branch Systems were segmented, and only people with the appropriate level of seniority could access them.[287] In order to access the system, there was an authentication procedure.[288] Systems or tools capable of more significant impact required further authentication.

261. It is my understanding that, in the case of management roles associated with management tasks like remotely accessing branch accounts, a physical token

---

[282] POL00401505
[283] See version 3.0 dated 17 December 1998 POL00400793; version 3.1 dated 18 February 2002 POL00400795; version 3.4 dated 18 February 2002 POL00400792 circulated to Warren Welsh and Andrew Gibson; version 4.0 dated 16 July 2002 circulated to Warren Welsh and Andrew Gibson; version 6.0 dated 8 August 2003 POL00400791 distributed to Warren Welsh and Andrew Gibson; version 7.0 dated 14 April 2005 POL00400790, distributed to Sue Lowther of Post Office
[284] POL00400799
[285] POL00400799
[286] POL00400799
[287] POL00400799
[288] POL00400810

WITN03680200

was required.[289] Administrative and 'super-user' access required two-factor authentication.[290] Access to the live environment required a high level of seniority and therefore a high level of authentication.

262. The **'Community Information Security Policy for Horizon'** was first issued on 8 June 2005.[291] It was a CCD which required Fujitsu to cooperate with Post Office and assist Post Office in complying with the standard set out in the policy, and to operate in accordance with ISO/IEC 17799:2000, Information Security Management: Code of Practice for Information Security Management as a baseline, together with other approved technical and procedural standards where appropriate. There was no specific requirement to undertake certification to ISO/IEC 17799:2000 but it was the domain suppliers' responsibility to identify and comply with the relevant standards. Successive versions of the document referred to the prevailing ISO standards. The Policy required that,

"*Access to Horizon information processing facilities must be controlled. There must be a demonstrable need for third party access. A risk assessment must be carried out to determine the security implications and control requirements for any forms of physical and electronic access by third parties.*"

263. The '**Horizon Security Policy'**, released on 24 February 2006, referred to the principles of the Security Architecture and Access Control Policy. It stated that a written request was necessary to gain access to systems and networks. This would be approved by the duty or owner of the business unit and retained

[289] POL00400810
[290] POL00394877
[291] POL00394583, v.1 6 June 2005; POL00397117v.2 22 March 2010; POL00397136 v.3 24 August 2010; POL00397343 v.4 13 October 2011.

WITN03680200

according to internal standards.[292] It required Fujitsu to maintain lists of individuals and their specific access rights by System Administrators who ensured that these reflected the principles in the Access Control Policy.[293]

264. The '**Security Management Service – Service Description'** refined this process in 2008 to specify that the individuals with Remote Access Rights – including TES-QA users, global users, and Audit and Engineer users – should be limited and stringently documented.[294] It stipulated that appropriate security measures should be applied to all remote access to Post Office systems, stating that:

"All remote access to Post Office Account systems, applications and data, i rrespective of access route, must be restricted to authorised users, and only to services, applications files or data for which those users are authorised. Such remote access must require verification and authentication of UserIDs, passwords, tokens, biometrics and where possible location details before connection is allowed."

265. It provided that active monitoring was to take place to ensure that no unauthorised or abusive access was occurring.[295] Periodic Checks were required to take place to identify inactive accounts and any user who changed roles or accounts was to be removed immediately.[296] The summary of these roles and the access permissions are contained in Appendix A of the Policy.

---

[292] POL00401642
[293] POL00401642; see v.7.1 dated 2 June 2009, POL00400809
[294] POL00397052
[295] POL00401642
[296] POL00401642

WITN03680200

266. It is my understanding that across the period that is the subject of question 3 of the rule 9 request, those who had sufficient power to remotely access the live environment included: application Support Managers;[297] Fraud Risk Managers (although only in pursuit of resolving fraud);[298] Business Function Auditors;[299] Security Event Auditors;[300] System Management;[301] SSC Support Managers;[302] SSC Support users;[303] non-dedicated Fujitsu Support Staff.[304]

267. The '**Post Office Account User Access Procedure**' was a Fujitsu document intended to establish the controls that applied to user access in order for Fujitsu to fulfil its contractual requirements to Post Office in this respect, for example version 4 of the document dated 18 October 2011 provided that "*only authorised individuals have access to the assets that their role requires*" and "*the access provided is managed, monitored, reviewed and controlled*".[305]

268. The '**HNG-X Architecture – Security Architecture'** set out the principles that the Security team operated under. It appears this sought to apply to the principle of 'Least Privilege' access, which was defined as "*that which is not explicitly granted is denied*" or a "*default deny*" stance which granted only the permissions necessary to carry out the action being performed.[306] This was echoed in the **Counter Architecture design** document.[307]

269. The **'Remote Support Secure Access Server High Level Design'** was a design document for the remote access server released on 24 October 2016.

---

[297] POL00401199
[298] POL00401199
[299] POL00400776
[300] POL00400776
[301] POL00400776
[302] POL00400776
[303] POL00397112
[304] POL00400667
[305] POL00225860, p.18
[306] POL00394877
[307] POL00398825

WITN03680200

It appears to have echoed the principle of tightly controlled access and authentication, stating that:

"*HNG-X users shall not have any access to add, modify, delete or execute any operating system or application files without first being properly authorised, authenticated and audited. Controls shall be in place to prevent this requirement being bypassed by any new or upgraded application or system build.*"[308]

270. I have also had sight of **the 'Systems Support Centre** (SSC) **Operations Manuals'**,[309] first released on 7 November 2000. Having reviewed these, it is my understanding that they show that the SSC had access to the live estate to correct data on the system when it had been corrupted in some way.[310]

271. I have also reviewed the **'End to End application Support Strategy'** release in July 2011 and which refined the role of the Support Services. This stated that; "*Direct access to live Post Office counters is currently only available to the SSC*" and "*depends on access to the SSN servers and the use of a passphrase which allows public key authentication to a fixed user on the counter*".[311]

[308] POL00400667
[309] POL00400840
[310] POL00400840
[311] POL00401116, p.11

WITN03680200

Conditions under which individuals could exercise access rights to remedy errors in transaction data and branch accounts

272. The Codified Agreement contained some provisions which had the effect of requiring:

a. authorisation; and

b. maintenance of records of access rights being used to remedy errors in transaction data and branch accounts.

273. It is my understanding that these obliged Fujitsu to maintain an audit trail that accurately recorded the details of amendments, remedies or new transactions. It is my understanding that these were further clarified in CCDs, particularly the '**Audit Trail Functional Specification**', to which the Codified Agreement cross-referred in every iteration.

Codified Agreement

274. **Original Codified Agreement**

a. **Schedule A16 Reference Number 804** stated that process of inserting the loss or gain transaction which negates and amends the original erroneous transaction must be carried out by the office manager within the office administration function.

b. **Schedule F01 Clause 4.4.1** stated that all transactions and actions undertaken in EPOSS shall be recorded in an audit trail by use of, and maintained by, the POCL Infrastructure Services.

WITN03680200

c. **Schedule G01 Clause 2.6.1.1.** stated that full logs of transactions and significant events within OPS shall be maintained and an audit trail of interactions with, and actions within, OPS shall be maintained.

d. **Schedule G01 Clause 2.6.1.2** stated that all data captured at an outlet either as part of a Counter Position Transaction or as an administration function shall form part of a unique transaction which shall be given a unique reference number by Riposte and details stored in the journal. The format of this journal entry shall vary according to the Transaction type but will typically contain: Post Office ID; Counter Position ID; Unique Transaction ID; Date; Time; User ID; Application; Transaction Details.

e. **Schedule G01 Clause 2.6.1.4.** stated that once data are stored in the journal, they shall never be altered and that new transactions should always be appended to the journal.

f. **Schedule G01 Clause 3.2.2** stated that the role of TMS shall be to provide a secure and resilient messaging and journalling service which shall support the transfer of data between OPS and POCL Client services, and the POCL Services.

g. **Schedule G01 Clause 3.4.7.1.** stated that Fujitsu should maintain a full audit trail of all TMS activity.

275. **2002 Agreement**

a. **Schedule 17 Clause 6.6.1.1** stated that all data captured at a Branch either as part of a Transaction performed at a Counter Position or as an administration function shall form part of a unique Transaction which shall be given a unique reference number by Riposte and details stored

WITN03680200

in the message store. The format of this message store entry shall vary according to the Transaction type but will typically contain: Post Office ID; Counter Position ID; unique Transaction ID; date; time; User ID; Application; and Transaction details.

b. **Schedule 17 Clause 6.6.1.3** stated that Once data are stored in the message store they should never be altered. New Transactions should always be appended to the message store.

c. **Schedule 17 Clause 7.2.2** states that the role of TMS shall be to provide a secure and resilient messaging and journalling service which shall support the transfer of data between OPS and Post Office Client Services, and Post Office Services.

d. **Schedule 18 Clause, 2.8.2** stated that the Audit facilities enable the recording of an operational audit trail and a commercial audit trail[312] as such terms are referred to in the CCD entitled "**Audit Trail Functional Specification**" (CR/FSP/006).

276. **Current Contract, Version 1 (2006)**

a. **Schedule B3.2 Clause 32.9.1** and **Schedule E Clause 107.1** stated that the Audit Support Facility enables the recording of an operational audit trail and a commercial audit trail as defined in the CCD entitled "**Audit Trail Functional Specification**" (CR/FSP/006)

b. **Schedule B4.4 Clause 62.2.2** states that the role of TMS shall be to provide a secure and resilient messaging and journalling service which

[312] These are, respectively, the audit trail associated with the operation of the services which make up the Horizon solution and the audit trail associated with that part of Post Office Account's internal commercial records to which Post Office Ltd's Internal Auditors or Agents may have access.

WITN03680200

shall support the transfer of data between OPS and Post Office Client Services, and Post Office Services.

c. **Schedule B5 Clause 8** states that Reconciliation Facilities are provided by the Business Capabilities and Support Facilities.

d. **Schedule B5 Clause 8** states that Reconciliation Facilities are provided by the Business Capabilities and Support Facilities.

277. Current Contract Version 11 (2016)

a. **Schedule B5 Clause 1.1.1** states that the role of TMS shall be to provide a secure and resilient messaging and journalling service which shall support the transfer of data between OPS and the HNG-X Service Infrastructure.

b. **Schedule D1 Clause 90.1** and **Schedule B3.2 108..9.1 and Schedule B5 Annex 2 Clause 7.1 and 7.2** stated that the Business Capabilities and Support Facilities provided by Fujitsu Services relating to the audit trail of transactions undertaken in branches are provided for in Schedule B3.2 and the provisions dealing with the operational audit trail set out in the CCD entitled "**Audit Trail Functional Specification**" (CR/FSP/006).

CCDs

278. The '**Access Control Policy'** stated that the changes that could be made by some individuals were subject to controlled conditions and authorisation procedures.[313] In **Version 1** of the Policy, released in April 1997, it was stated that the operational management of the machine facilitating the remote access

[313] POL00400776

WITN03680200

would confirm the need for access.[314] Similarly, **Version 2** of the Access Control Policy released on 16 July 2002, stated that updates to code or data by support staff was to audited.[315]

279. The '**Audit Trail Functional Specification'** set out Fujitsu's obligations to maintain and provide access to audit trails. **Version 3** released on 1 July 1999[316] provided that:

> "*1.1.1 The operational audit trail includes that generated by the mainstream operational services and the Reconciliation Exceptions Database (RED)… The RED provides an auxiliary audit trail which separately covers the treatment of exceptions encountered within the mainstream operational services.*"

> *"3.1.1 RED is free-standing from the mainstream Pathway Solution. It is a record of the activities undertaken by the Pathway Customer Service Business Support Unit to make necessary adjustments to transactions, typically to effect accurate reconciliations.*"

280. It is my understanding that this meant that reconciliation exceptions – for example, transaction corrections – should have been separately captured within the audit trails provided for. In a subsequent version of this document released on 15 October 2001, the term 'RED' had changed to 'BIMS'.[317]

[314] POL00400810
[315] POL00400776
[316] POL00401619
[317] POL00393978

WITN03680200

281. The SSC '**Operations Manual'** set out expectations for the processes that individuals were to follow for "*every change to the live system*."[318] This was echoed in the **Operations Manual for the Customer Services Directorate**.[319] The procedure required a Duty Manager, Problem Manager, Business Support manager or SSC Staff Member to complete an Operational Correction Request Form, which would document the affected part of the system. The process required that changes to the live system should only be made in the presence of two people. The OCR form required to be signed, sequentially, by the individual who made the change and the two people who witnessed them making it. I note that in **Version 4** of the Document, released on 16 July 2002, the requirement to submit an Operational Correction Request seems to no longer apply, although two staff members were still required to be present.[320] The Operations Manual also repeated provisions set out elsewhere in respect of security policy, as it stated;

"Security policy mandates that all users requiring access to the live system have to be approved by CS Security. This is a fundamental security access control requirement. The procedure involves the completion of an application form, which is authorised by the individual's Business Unit Manager. This is forwarded to CS Security who validates the request and sends to ISD Operations via the ISD mailbox for activation on the system."[321]

282. Version 7 of the '**Access Control Policy**' dated 14 April 2005 stated:

[318] POL00400840; POL00400835
[319] POL00401505; POL00400835
[320] POL00400776
[321] POL00400835, 3.13.27.1

WITN03680200

a. *"Note that no application support users have access to Post Office counter systems except as allowed for in 4.5.5.2 below.*

b. *4.5.5.2 SSC access to the counter estate via SSH and may download data from the Data Centres to an appropriate test rig where this is required to assist in diagnosing application problems and testing new software to fix the prob*lem.

c. *4.5.5.3 Support users should have only read access to the supported systems, except for: SSC support managers (not normal SSC support users) "correcting" data under controlled conditions. (Data may need to be corrected where it has been corrupted by faulty code.) Correction of data must be subject to agreed authorisation procedures*.

d. *4.5.5.4 In all cases, updates to code or data by application support staff require two staff to be present when the change is made and all such changes to be audited, identifying what has been changed (before a*nd *after values) and the individual who made the change."* [322]

283. The '**Horizon Security Policy**' released on 24 February 2006 provided that Line Managers must have implemented a formal process for requesting, authorising, granting, reviewing and revoking access rights to Post Office Account business information, systems and networks. Business Managers were also subject to this responsibility.[323] The policy provided that:

"Security audit trails are required to provide traceable evidence of all activities affecting information system, application and network resources. This must include both transaction and system audits. The audit trail must include all

[322] POL00400790, p.39-40
[323] POL00401642

WITN03680200

violations and exceptional events as required by both the owner and audit functions. The audit logs must be retains for a minimum period commensurate with the requirements of the system or any regulatory authorities."[324]

284. Several design documents also emphasised that the maintenance of audit logs was a condition of the exercise of accesses to remedy errors in transaction data and branch accounts. For example, the **'Security Architecture'** documents stated: "*all actions performed on the system will be recorded to establish an audit trail*" and specifically stated that 'super-user' access was to be audited.[325] They specified that the person who made a specific change was meant to be identifiable.[326] In Version 6 of the document, released on 12 July 2017, a PEAK reference was required to be part of the audit trail which would have ensured that the action could be tied to a specific Incident or Problem.[327]

285. The '**End to End Application Support Strategy'** released on 28 July 2011, stated that the teams that had the ability to change data like the SSC were prohibited from also editing the audit trail. The document went onto state that:[328]

"The audit servers provide a full audit trail of all information on the HNGX system. In order to ensure that this audit trail is irrefutable the teams which have the ability to change data (i.e. SSC) must not also have the ability to change the audit trail. For this reason, Audit server 3rd line support rests with the Audit development team and not the SSC."[329]

---

[324] POL00401642, p.58
[325] POL00394877
[326] POL00397112
[327] POL00400323
[328] POL00401116
[329] POL00401116, p.11

WITN03680200

286. I have reviewed a number of documents, from which my understanding is that, from 2008, the stringency of the requirements that access to the live system be auditable was reduced.

287. I noted firstly that the '**Remote Support Secure Access Server High Level Design**' Version 2 issued on 13 May 2008 re-drafted a clause about audit, so that it read as follows:

"Although no active command logging or keystroke logging is done but we are keeping the record of people logged on to SAS (SSN) server through double authentication and OS security policies for state servers. Security policy is implemented to raise alert when any file is copied or deleted to SAS (SSN) server. Also no user account is allowed to install any software on SAS (SSN). FTP folder will be maintained manually by SSC team."[330]

288. Version 1 of the same document, issued on 10 January 2008, stated that; "*All access through the Secure Access Server should be audited. A command logging service will be provided to create audit logs of all support sessions.*"[331] My understanding is that this preserved the need for auditing of which users accessed records of branch transactions but it meant that there would not be auditable records of what those users did. My understanding is that this design document is the origin of the documents that became known as the '*Privileged User Access'* logs (or **'PAU logs'**).

289. Version 2 of **'HNG-X Architecture: Security Architecture'**,[332] issued on 8 January 2009, stated, in Paragraph 5.1.1 that: "*All access to the SAS Server is*

[330] POL00396665, clause 3.1.2
[331] POL00395680, clause 4.1.2
[332] POL00397112

audited though command line auditing of SSH sessions has been removed." This differs from Version 1[333], issued on 16 February 2007, which stated at Paragraph 5.8.3 that "*Auditing is turned on including command line auditing for super-user access via SSH.*"

290. The difference between the two versions seems to me to be potentially significant because SSH facilitated the secure link between the SSC and the counter infrastructure. The command line was the means through which changes could be made to transaction records. My understanding has been reinforced by Version 2 of the '**Remote Support Secure Access Server High Level Design**' (in effect when Version 2 of the Security Architecture CCD was issued) which states that the SSH server "*will provide a secure link for support access*"[334] and identified[335] as a risk that the command line auditing had not been developed in time for the release of the HNG-X System.

291. It is my understanding that at the same time there was recognition within the SSC that the tools in place for making balancing transactions were powerful and not without risk. The Fujitsu document '**Branch Database High Level Design**', Version 1 of which was issued on 17 November 2009,[336] described the Balancing Transaction tool BRDBX015 as follows:

    a. *"There is a requirement that the SSC will have ability to insert balancing transactions into the persistent objects of the Branch Database. There are reasons for SSC having to do so e.g. to rectify erroneous accounting*

[333] POL00394877
[334] POL00396665
[335] POL00396665, p.29
[336] POL00397089

data that may have been logged as a result of a bug in the Counter / BAL.

b. *Any writes by the SSC to BRDB must be audited. The mechanism for inserting a correction record must ensure that the auditing of that action performed must be atomic. There also needs a level of obfuscation to ensure that the audit mechanism is robust.*

c. *The above-mentioned requirements suggest that there is a need for a correction tool to be delivered which performs the correction, audits it and saves both changes.*

d. *A simple low-cost solution for the tool is to provide a Linux shell based utility, which calls a PL/SQL package to perform the changes. The package will allow inserts to the following transactional tables in the Branch Database Live schema with the exception of the Message Journal. All inserts will be audited in the table BRDB_TXN_CORR_TOOL_JOURNAL."*[337]

"7.2.12.6 PROCESSING DETAILS

e. *Warning: The use of this powerful tool has inherent risks. If the SQL statement is incorrect or badly written, it is possible to cause unintended consequences, some of which may cause serious problems to the Branch Database. It is expected that only a small number of skilled staff will run this tool and that they will have detailed guidance as to when and how to use the tool.*

f. *The correction tool places a number of constraints on the contents of the transaction file. These are necessary in order to provide a defined*

[337] POL00397089, clause 5.7.2

WITN03680200

baseline upon which it can base its operation. If any of the constraints are violated then validation will detect it and abort the run with a meaningful error message."[338]

Regular mechanisms of monitoring

292. It is my understanding that monitoring the usage of access rights was therefore intended to be a key part of the security architecture. Throughout the relevant period, the function of monitoring Fujitsu's operational-level access to the system was outsourced to Fujitsu's security team, who would in turn report to Post Office. Post Office treated the Fujitsu security team as independent of, and able to monitor, the Fujitsu SSC employees. I understand from discussions with colleagues that, at the time, it was viewed as an unremarkable aspect of the *'software as a service'* model, and this is consistent with my own knowledge and experience of working within the IT community during the same period. It meant that, in effect, Post Office was dependent on Fujitsu for the provision of information about the extent to which Fujitsu was complying with its contractual obligations around privileged access rights, including the auditing and supervision thereof.

293. The service that Post Office commissioned from Fujitsu in respect of the security for the Horizon system was set out in the CCD '**Security Management Service: Service Description**'[339], Version 5 of which was issued on 4 April 2014. Versions[340] of this document provided, among other things, that Fujitsu should liaise with Post Office in accordance with the CCD '**Post Office HNG-X**

[338] POL00397089, clause 7.2.12.6
[339] POL00401510, v.5 dated 4 April 2014
[340] POL00401509, v5.1 dated 3 March 2015

WITN03680200

Account Information Security Policy,' run monthly internal Information Security Management Reviews (**ISMR**) providing agreed monthly reports; and attend monthly customer ISMF meetings, providing agreed monthly reports.

294. A **Management Assertion** from February 2013[341] (contained within Fujitsu's description of the IT infrastructure services supporting Post Office 's POLSAP and HNG-X applications throughout the period 1 April 2012 to 31 December 2012), stated that: "*Controls exist to provide reasonable assurance that remote access is appropriately restricted to authorised personnel.*"

295. In November 2013, a meeting took place between the Post Office Information Security and Assurance Group (ISAG) and Fujitsu, the minutes[342] of which record that it was intended:

"To record and review any changes to privileged user access on a monthly basis and to undertake a full review twice a year. It was previously agreed that a User review would be undertaken at this meeting. However the information was not made available at the time of this meeting."

296. Fujitsu's **Management Assertion** from February 2014[343] (contained within Fujitsu's description of the IT infrastructure services supporting Post Office's POLSAP and HNG-X applications throughout the period 1 April 2013 to 31 December 2013), repeated the previous year's statement that; "*Controls exist to provide reasonable assurance that remote access is appropriately restricted to authorised personnel*."

[341] POL00031407
[342] POL00031407
[343] POL00398087

WITN03680200

297. I have reviewed an e-mail from February 2014 from Alastair Kay at Fujitsu to Kathryn Alexander at Post Office concerning access to information and branch logs, in which Mr Kay stated that; "*The data from the branches are saved on the Central dbase. Therefore Support are the only team who have read access to the data for Logs etc.*"[344]

Internal and external mechanisms of monitoring – audits and reports

298. The management summary of an audit of the Horizon Data Centres and Belfast Operations by ICL Pathway in 2001[345] found (amongst other things) that:

"Non-approved tools are being used to remotely administer the live estate resulting in an inability to audit individual user activity as is required by agreed policy. Alternative options are already being considered by Pathway to address this issue. User account administration should be reviewed and enforced to obviate the need to by-pass approved account policies by using Administrator privilege."

299. Ernst & Young LLP (**'EY'**) then prepared an Audit Report in respect of Royal Mail for the year ended 30 March 2008. That report included the following comments in relation to Royal Mail's IT processes and the robustness of its IT infrastructure:

a. *"Following the challenges experienced in performing our IT audit in prior years, the audit process was greatly improved … as the ownership within*

[344] POL00401632
[345] POL00394026

WITN03680200

the Group IT function for managing third party suppliers and delivery of audit information requests becomes clearer as individuals are more accountable.

b. *"The most significant finding related to the SAP system. Whilst we are satisfied that the mechanism for granting access rights to Royal Mail employees is appropriate, we identified 61 third party programmers at the year end [sic] (and a further 76 during the year) who had unlimited access to the Group's SAP systems as a result of having the all powerful [sic] 'SAP-ALL' profile for which there was no audit log or other such mechanism to monitor the use of this access"*.

c. *"In our experience, where IT systems and processes are outsourced, it is not unusual for third parties to have super access to an organisations systems in order to discharge their contractual responsibilities. However, the number of individuals with these rights are usually relatively few and they are known to the company. Where it is necessary to provide this level of access rights to additional contractors, authorisation is required for the company prior to execution by the supplier*".

300. The Audit report identified two specific examples of third-party access including the following comment in relation to POL-MI, MDR / FRS: *"A limited set of users have access to manipulate data as it is loaded into these databases. Our extended procedures were designed to address the risks arising from this and the ineffective change control issue for SAP-ADS.*

WITN03680200

This extended testing also represented our alternate approach to Horizon."[346]

301. It is my understanding that the Royal Mail Holdings **Audit and Risk Committee** meeting in March 2008 was informed of a presentation to the Royal Mail Holdings Board in which it was explained that the IT capabilities of Royal Mail were "*inadequate for the current and future environment*".[347] Concerns appear to have included those relating to system access. The Committee decided the IT control environment should be a regular item at future Audit and Risk Committee meetings so that the Committee could be updated on progress.

302. The Royal Mail Holdings' **Audit and Risk Committee** meeting of May 2008 summarised EY's findings as follows: *"Following the challenges experienced in performing the IT audit in prior years, the audit process was greatly improved, as the ownership for managing third party suppliers and delivery of audit information was much clearer and individuals were more accountable. The most significant finding had been the unlimited access to the SAP system by third party programmers. The findings were consistent with the broad themes and challenges in relation to the Group's IT environment presented to an earlier meeting of the Committee.*"[348]

303. The Committee concluded it could not reach firm conclusions about the control environment until the IT strategy had been developed further and it requested an update at the **Audit and Risk Committee** meeting in September 2008.

[346] POL00396456
[347] POL00396009
[348] POL00396455

WITN03680200

304. It is my understanding that a presentation was prepared for the September 2008 meeting which identified access control as a critical point of focus. The steps taken to address this weakness were described as disk encryption and firewalls.[349] The minutes state a further update would be provided in March 2009 but, pursuant to the searches that have been carried out for documents to assist me in responding to the rule 9 request, I have not been able to find any minutes from that month.

305. In May 2010, EY reported: *"Whilst some improvements were noted in the POL IT audit process, we continue to face difficulties in obtaining accurate information from Fujitsu, one of the outsourced providers of POL IT systems."*[350]

306. In was further stated by EY that; *"POL has made significant changes to its IT environment in 2010, resulting in the inclusion in scope of the Credence application for the first time, replacing POL-MI and the Reference Data System. During 2010, POL also worked with Fujitsu to deliver a new version of the Horizon application used at, and in support of, Post Office branches. This new version of Horizon was also included in scope."*[351]

307. EY also referred to difficulties in performing IT general control procedures with Fujitsu in 2009 and noted these difficulties continued, reporting that; *"While the controls operated by Fujitsu on behalf of Post Office were appropriately designed an exception was noted in the revocation of user access. Access was immediately revoked by Fujitsu when this was identified."*[352]

[349] POL00396890
[350] POL00030261
[351] POL00030261
[352] POL00030261

WITN03680200

308. As part of the Royal Mail Holdings plc audit conducted by EY,[353] a **Management Letter** for the year ended 27 March 2011 was prepared which said as follows:

a. *"In POL, our audit identified significant IT control weaknesses, which in our view reflects a need for improvement by the outsource provider Fujitsu but also a change in approach on the part of POL. However, we ultimately obtained mitigating audit evidence to rely on the IT control environment."*

b. "*… there is no one Fujitsu or POL person who has full knowledge of POL's end-to-end processes or access to documentation and other evidence to support the operation of key controls which result in certain information which we could consider routine not being available*".

c. "*The main area we would encourage management focus on in the current year is improving the IT governance and control environment. Within the IT environment our audit work has again identified weaknesses mainly relating to the control environment operated by POL's third party IT suppliers. Our key recommendations can be summarised into the following four areas:*

   i. *Improve governance of outsourcing application management;*

   ii. *Improve segregation of duties within the manage change process;*

   iii. *Strengthen the change management process; and*

[353] POL00030217

WITN03680200

iv. *Strengthen the review of privileged access.*" [354]

309. The report noted that *"the recommendations we have made in this report should be seen as refinements rather than fundamental control deficiencies in comparison*."[355]

310. Section 3 of the report, which concerned strengthening the change management process, which had been deemed by EY to be a high priority area, included a review of and raised concerns in respect of privileged access to IT functions.

311. The first of these concerns was; "*We reviewed privileged access to IT functions including access to user administration functionality across all in-scope applications and their supporting infrastructure. Our examination revealed*:

312. The second was; *[…] HNGX - There are inappropriate system privileges assigned to the APPSUP role and SYSTEM_MANAGER role at the Oracle database level on the Branch Database server (BDB) supporting HNGX*;

313. The third was; *[…] System privileges assigned to the APPSUP role and OPS$TPS account are inappropriate*.[356]

314. The fourth was; "*Unrestricted access to privileged IT functions increases the risk of unauthorised/inappropriate access which may lead to the processing of unauthorised or erroneous transactions".*[357]

[354] POL00030217, p.3
[355] POL00030217, p.3
[356] POL00030217, p.33
[357] POL00030217, p.34

WITN03680200

315. The fifth was; "*There are no monitoring controls in place for privileged IT access to HNGX.*"[358]

316. The 2011 **Management Letter** included a number of recommendations for Post Office in relation to privileged access including that "*management conducts a review of privileged access to IT functions across all in-scope applications and their supporting infrastructure to determine whether the level of privileged access granted is appropriate*" and, "*Management should consider the implementation of a POL owned periodic review of appropriateness of access to in-scope applications and their supporting infrastructure*" and, "*The above review should include all user accounts including those privileged user accounts owned by IT and vendors.*"

317. Post Office "**Management Comment**" in the 2011 Management Letter noted that "*work has commenced on the strengthening of the change management process*" and noted a number of future steps to be taken including "*POL to review the current BAU governance to ensure the change management principles are being applied and monitored*" and "*reporting and evidence to be agreed regarding BAU reports of Privileged Access abuse to provide POL with the assurances they require.*" "*Fujitsu senior management … to review rights of their staff and their appropriateness every quarter. Quarterly BAU Assurance reports to POL concerning reviews that have occurred across the account will be governed by the Audit Control Governance Board.*" There are no harmful events in relation to change management and permissions noted in the 2011 management letter nor is there an instance of irregular or unauthorised remote access recorded.

[358] POL00030217, p.36

WITN03680200

318. EY prepared their **Audit Results Report** for the year ended 27 March 2011 for Royal Mail Holdings Plc in May 2011.[359] That report made a number of observations in relation to IT control weaknesses, noting that (amongst other matters) in so far as POL-SAP was concerned there were:

a. *"Accounts with access to both develop and deploy changes to the live environme*nt";

b. There was: "*Access to deploy changes for inappropriate individuals/leavers*".

c. There were "*multiple generic accounts with highly powerful privileges.*"

d. There was a "*lack of periodic review of appropriateness of user access.*"

319. In relation to HNG-X, additional concerns were raised, which included the following:

a. There were "*developers with access to migrate changes to the live environment.*"

b. "*Leavers with access to promote changes to the live environment not being removed*."

c. There was evidence of "*lack of periodic review of appropriateness of user access*."

d. There was evidence of "*passwords for privileged generic accounts being shared with multiple users.*"

320. In response, it is my understanding that there was a de-brief session between Post Office and Fujitsu regarding the "*difficulties faced during the audit.*" Lesley

[359] POL00030217, p.36

Sewell engaged "*...with the Fujitsu account leader to highlight Post Office's desire to implement a required controls framework and explore options for the conduct of the audit in future*". From these discussions, Post Office understood that "*...Fujitsu has accepted that control improvements are required and has initiated a project to address the security issues.*" What were described as "*high-level action plans*" were agreed by Fujitsu, Post Office and EY to improve the audit process for the following year.[360] Post Office established an audit steering group to implement EY's recommendations.[361]

321. It is my understanding that, in September 2011, a '**Post Office Board Paper – POL IT Audit Update,'** presented by the then Chief Operating Officer, explained that an **Audit Steering Group** had been established for IT related audits which he said provided the appropriate level of governance and oversight to ensure that the audit actions were completed as agreed and the alignment of all Post Office's compliance audit requirements. The paper explained that a project team had been established within Fujitsu to manage all activities which were on target for completion by end of October, within which Fujitsu had completed two of the recommendations, namely strengthening the change management process and improving the problem and incident management process. He reported that, in light of the finding that in respect of the level of oversight and assurance of control processes within Fujitsu, Post Office were "*working with Fujitsu to build a reporting process to ensure visibility of Fujitsu's control environment is transparent to POL through regular reporting activity*." He noted that five of the recommendations relate to user management and

[360] POL00238126
[361] POL00029438

WITN03680200

access rights to Post Office's systems, and said, "*A complete review of this area is underway and is on target for completion*". He said Post Office were working on three actions independently of Fujitsu, which refer to improved user management controls within the Post Office finance system for cash services, a review of the testing process for maintenance / business as usual ("BAU") changes (to ensure that a consistent approach exists and is followed, with regular audit to monitor compliance) and the creation of a central store of approvals.

322. I have also had sight of email correspondence between Neil Lecky Thompson (Head of Programmes and Planning, Post Office) to Lesley Sewell and Sarah Hall dated 21 March 2012 which contained a summary of Post Office's internal views of the issues raised in the audit and made reference to a lessons-learned exercise being conducted.[362]

323. In the summary described above, some recommended management responses to findings made in the report. However, I have not been able to establish the extent to which these findings were ultimately implemented. They were as follows:

Finding	Recommended Management response
Strengthen user admin process: [1] 4x HNG findings – 2x findings – resolved through initiation of revised process; [2] 4x SAP	"*As part of the improvement process, and due to findings from last year's audit a standardised access control management process has been implemented by Fujitsu for both HNG*

[362] POL00142943 (email) and POL00142944 (attachment entitled "Management Response and summary of E&Y Financial Audit findings 2011/12")

WITN03680200

findings all in Cash Centre – responsibility of CC Managers	*and POLSAP (excluding Cash Centres). This process requires further evaluation to assess performance, but has already been proven to catch outstanding anomalies. Mitigating controls are in place through the use of iKeys and issuing procedures.* *Fujitsu HR are now part of the process in access revocation.*"
Review of privileged access: [1] SAP – 2x findingsPOL Information Security – to assess whether appropriate to shared service environment; and [2] HNG – 2x findings POL Information Security – to assess whether appropriate to shared service environment.	The 'Recommended management response' is largely a copy of the above but additionally states that "*Reporting and evidence has been standardised in BAU reports for Privileged Access utilisation. As part of the iSMF BAU process management reviews assess adequacy and regularity of the controls in place. POL Information Security to review appropriateness of access against best practise and centre of excellence models.* *E&Y to provide amended RAG status*"

WITN03680200

324. Shortly thereafter, on 23 March 2012, Post Office's **Internal Audit and Risk Management Report**, which was entitled *"Internal Audit & Risk Management: Review of Key Systems Controls in Horizon"* was circulated internally.[363] In that report, it was stated;

a. "*Unrestricted access to privileged IT functions increases the risk of unauthorised/inappropriate activities which may lead to the processing of unauthorised or erroneous transactions.*"

b. *"We recommend that management conducts a review of privileged access to IT functions across the in-scope applications and their supporting infrastructure to determine whether the level of privileged access granted is appropriate. Where access is deemed to be inappropriate, this access should be revoked immediately."*

325. In May 2012, the 2012 **EY Audit Report** stated that: *"In conjunction with our IT specialists, we have assessed the manage change and logical access IT controls to be ineffective, which was the same conclusion we reached in the prior year. However, through additional compensating testing we have been able to rely on the IT systems supporting the POL financial statements."*[364]

326. A presentation to the **Risk and Compliance Management Committee** on 14 May 2012[365] stated (amongst other matters) the following in relation to privileged user access:

---

[363] POL00142948. The report is noted as having been circulated to the following individuals: Susan Crichton, Legal and Compliance Director, Christopher Day, Finance Director, Kevin Gilliland, Network and Sales Director, Dave M King, Senior Security Programme Manager, Neil Lecky-Thompson, Head of Programmes and Planning, John Scott, Head of Security, Lesley Sewell, Head of IT and Change, Paula Vennells, Managing Director, Mike Young, Chief Operating Officer, Alice Perkins, Chairman.
[364] POL00143038
[365] POL00397495

WITN03680200

a. *"Privileged user access*

b. *Reduction of number of privileged users from last year*

c. *However still privileged access exists with limited controls in particular in POL SAP*

d. *Key actions:*

e. R*eview to assess feasibility of devolving SAP_ALL by 30/08/2012*

f. *Following review aim to ensure privileged access is given on a strict business need, such as incidents and change requests raised and where given effective monitoring in place by 30/09/2012*

g. *User admin process*

h. *Approval of users access not always evidenced*

i. *Removal of some users not always timely*

j. *Key actions:*

k. *Review of user admin process regarding approval and retention in conjunction with Fujitsu to assess feasibility and need for a monitoring process by 31/08/2012*

l. *Finding to be reviewed and next steps agreed by POL and POA (Fujitsu account management) by 31/10/2012"*

327. It is my understanding that a final draft of the **"E & Y Post Office Limited: Control themes and observations for Year ended 25 March 2012"**[366] contained a number of recommendations, to which Post Office Management responded. The recommendations were that Post Office Management should (i) conduct a review of privileged access of IT functions to determine whether

[366] POL00143524 (covering email from Sarah Hall (Financial Controller, Post Office) to Rod Ismay and Lesley Sewell) and POL00143525 being the report itself.

WITN03680200

the level of access is appropriate; and (ii) where access is deemed to be inappropriate, this access should be revoked immediately. It was also stated that "*Management should implement monitoring controls to help ensure that controls operated by the third party service providers are in place and are in operation, for example, monitoring of appropriateness of access to privileged users/profiles.*"

328. In response, Post Office is recorded as having stated,[367]

> *"This observation and recommendation, repeated in previous audits, has been successively addressed by increasing levels of control. Since the last audit the use of Generic Privileged Accounts is monitored continually by Fujitsu. The granting of this privilege must be justified; is time-bound and is reported monthly to the POL Information Security Management Forum (ISMF) for approval by the head of Information Security. In addition, where users have access to this privilege, their ability to 'SUDO' (switch privileges inside user session) is additionally monitored. As for previous years there is a continuing need for certain key system activities to be executed by these admin teams with these privileges. For out of hour's support it is not possible to predict the privileges required for support, therefore the use of elevated privileges is justified. […]Further additional controls do not appear to be justified. However the rigor of the monthly check at the ISMF will be tested to ensure it is adequate, if not steps will be taken to optimize the checking of these accounts."*

[367] POL00143525, p.13-14.

WITN03680200

329. Post Office went onto state that; *"The issues around privileged access are focused on the possibility that a privileged user may abuse their access. Post Office believes that the existing process provide sufficient transparency and accountability to deter such activity. Post Office accepts that deterrence is not as strong as prevention. Consequently, Post Office's attention will address enhancing the process to ensure that lapses in record keeping cannot easily occur in the future; and that attention will be given to enhancing this accountability and transparency where possible."*

330. A meeting of the **Risk and Compliance Committee** in September 2012 received a summary of the Management Control audits performed over the previous two years by EY. It recommended that controls in place were sufficient to mitigate the existing low risk exposure. It proposed that the Committee should agree the acceptance of the risks associated with the audit findings.[368]

331. A report was made to the **Risk and Compliance Committee** in November 2012 providing an update on the progress of the IT audit rectification plan following the 2011/12 EY Audit.[369] The report noted the completed actions from the EY report (which included those in relation to privileged access, being:

a. review of privileged access to determine if the level of privilege is appropriate;

b. consider implementing monitoring controls to ensure that robust security practices are in place; and

[368] POL00397878

[369] POL00397899. Full list of recipients: Jonathan E Hill, Lesley J Sewell, Malcolm Staite, Martin Moran, Nigel Tuppen, Susan Barton, Susan Crichton, Dave Pardoe, Andy J Jones, Simon Baker, Mark Pearce, Amanda Brown, Glenda C Hansen, Gina Gould, Kelly Marie Reeder, Suzanne Jolley.

WITN03680200

c. implement a Post Office owned periodic review of appropriateness to determine if there is any inappropriate access.

332. The report also noted a number of actions from the EY report that required endorsement by the Committee including that: "*there is a risk that people make unauthorised changes to the systems and affect our data integrity.*" The steps taken in mitigation were listed, as was the basis for why these were thought to be acceptable. It is my understanding, from my review of this report, that Post Office believed at this time that the controls in place were:"*… adequate to mitigate the risk of unauthorized changes, they are: 1. Post Office reviews all privilege access requests; Usage is monitored and reviewed. 3. Changes to IDs are reported immediately to the Post Office. 4. Periodic reviews take place to re-approve all such IDs.*"[370]

333. In December 2012, Post Office '**Internal Audit & Risk Management - Horizon System Control Assurance Review'**[371] was carried out to assess the degree to which the issues raised in the 2011/2012 EY Management Letter had been addressed by Post Office's management. The review reported that: *"Generic privileged accounts remain in use on Horizon by Fujitsu. A paper was presented to the November POL Risk and Compliance Committee where any residual business risks associated with this control were accepted by IT and Change on behalf of the business. Implication: Accountability in the application may not be fully controlled, leading to a risk of inappropriate activities being undertaken within the system".*

[370] POL00397899
[371] POL00398154

WITN03680200

334. An **Audit and Risk Committee** meeting in May 2013 recorded the following in its minutes that: *"They [Ernst & Young] congratulated the business for the improvements in the IT controls, stressing that this had been driven by good governance and a tight control framework. The co-ordinated audit between Finance and IT was highlighted as a success and Sarah Hall and Lesley Sewell were to be thanked for their input."*[372]

335. I understand that, in early 2013, Post Office agreed with Fujitsu that at Fujitsu's cost they would separately engage EY to assess its controls and produce a ISAE 3402 report, in order to provide a description of Fujitsu's total IT support processes and controls operated in managing the Post Office Account for Horizon on-line and POLSAP.[373] The report produced on 4 March 2013 was entitled, "Fujitsu and E&Y: ISAE 3402 report: Description of Fujitsu's System of IT Infrastructure Services supporting Post Office Limited's POLSAP and HNG-X applications".[374]

336. This was a very detailed report which gives the reader the overall impression of a robust system with substantial controls in place, which had been spot tested and validated by EY. It referred to the *"Managed Service Change (MSC) operational change"* and said that "*In summary, MSC is a Fujitsu toolset that allows a securely accessed, time stamped auditable system to record change, provides Service Delivery Units and Service owners with audit trails and gives reasonable assurance that modifications to software and infrastructure are assessed for risks & impacts. The changes are authorised by the Service owner and Change Manager, are tested by appropriate methods. Teams are approved*

[372] POL00397990
[373] POL00137294
[374] POL00026621

WITN03680200

to be deployed to a live environment subject to testing results, they are implemented by the authorised and approved teams and the changes are documented into new or existing documentation."

337. The report further explained that, "*The principle of "least privilege" is used to restrict the access rights of users whether human or non-human*" and the role of the "*The Information Security Monthly Forum (ISMF) [as] a formalised monthly forum where Post Office and Fujitsu Security production risk and control concerns / issues are raised and progressed with the necessary stakeholders*" who have a role in reviewing the "Active Directory User Access Review" of users and their associated privileges. It explained that certain users within Fujitsu had "*access to administer POL's databases*" which were said to be "*restricted to appropriate Fujitsu personnel required to have this level of access by their role.*" The section went on to explain that "*Database access control also requires individual role-based accounts for each class of user, both for controlling the actions a user can perform and for helping to ensure administrative and other actions are traceable to an individual to provide a valid and informative audit trail.*" It stated that controls existed to provide reasonable assurance that remote access was appropriately restricted to authorised personnel.

338. My understanding is that this report was made available to Post Office and that Post Office relied upon it as assurance of the security and integrity of the exercise, monitoring and auditability of Fujitsu's access rights. The '**EY Post Office Limited: Report to the Audit and Risk Committee 2012-13 Audit Results Report**' dated 14 May 2013[375] stated that; "*No significant findings were*

[375] POL00144637, p.197

WITN03680200

noted in the ISAE 3402 report commissioned by Fujitsu, and we have therefore been able to rely upon it for our IT audit. We were also able to place reliance on the effectiveness of automated controls within HNGX and POLSAP for financial statement audit purposes."

339. I have reviewed an e-mail sent on 24 April 2014 enclosed a PowerPoint presentation entitled **'Follow Up Review of Key System Controls in Horizon'** prepared by Internal Audit & Risk Management for presentation to Post Office[376], which stated that: *"Through consultation with Fujitsu, POL management have confirmed that privileged generic accounts are controlled and will not be replaced with individual accounts. The residual business risk associated with this control was accepted by IT and Change at the November POL Risk & Compliance Committee on behalf of the business."*

340. Subsequently, in 2014, it is my understanding that Deloitte were engaged at the request of the Post Office Board to conduct a desktop review of certain Horizon matters raised in the context of the Initial Review and Mediation Scheme.

341. At the Board meeting on 30 April 2014, the outcome of this review by Deloitte (referred to as **Project Zebra**) was discussed.[377] Deloitte's proposal paper for Phase 2 of Project Zebra was stated to have been devised to assist Post Office in answering questions that included: "*what assurance could be provided over how the system records and maintains the transaction logs*" *"...in the context of specific allegations regarding non-traceable, "phantom" transactions existing in Horizon".*

[376] POL00398154
[377] POL00021524

WITN03680200

342. In May and June 2014, Deloitte produced two documents for Post Office as part of Project Zebra entitled '**Horizon: Desktop Review of Assurance Sources and Key Control Features**' and an accompanying '***Board Briefing***'. It is my understanding that Deloitte did not test any of the relevant Horizon features and were not required to revalidate the work supplied to them.

343. The Board Briefing notes 2 means by which appropriately authorised Fujitsu users could theoretically remotely alter branch transaction data which were as follows:

a. through the processing of a certain type of centrally generated transaction, 'Balancing Transactions'; and

b. database access privileges allowing the theoretical deletion and replacement of data in the Audit Store. Deloitte observed that this was a matter contrary to Post Office's then understanding.[378]

344. On 4 June 2014, Deloitte produced a Board Briefing[379] following their '**Horizon: Desktop review of assurance sources and key control features**' report dated 23 May 2014. The briefing stated that:

a. *"POL is reliant on the features identified being implemented and operating as described. In particular evidence based testing is not available relating to relevant business processes and inbuilt controls, other than access controls*.

[378] POL00399614
[379] POL00030451

WITN03680200

b. *Assurance evidence no longer remains available from the original implementation project. POL's historic comfort is therefore sourced from assertions from POL and Fujitsu staff*.

c. *Data is permanently deleted from the Audit Store after seven years. We understand that some allegations relate to periods older than seven years*.

d. *It is possible for Fujitsu staff with suitably authorised privileged access to delete data from the Audit Store.*

e. *Sub-postmaster reports showing detailed transactions of their Branch are limited to the current accounting period and part of the prior accounting period, and are not drawn from the Audit Store.*

f. *Digital signatures and digital seals are a key control feature underpinning the integrity of Horizon. In considering the design of the Horizon Features, we would expect that there would be activitie*s or *testing performed to verify it had been implemented as designed; the need for those controls is borne out by the fact that one of the features has not been implemented as expected."*

345. A Post Office action summary from June 2014[380] referred to the risk of someone with remote access being able to delete data. I have not been able to establish if this summary was seen by the General Counsel team. The summary proposes setting up a "Horizon Management Council" with representatives from Post Office and Fujitsu and notes that:"*… it was possible for 'someone with privileged access to delete data from specific areas of Horizon. This is always*

[380] POL00401635

a risk with individuals using admin or power user accounts and is a persistent risk, one that needs to be catered for in almost any organisation. Due to the sensitive nature of the information contained in the databases, monitoring of those databases should be put in place using technology to detect and record deletions and administrative changes to the databases. If possible, alerts should also be generated for mass deletions and high level risk changes to database schemas."

346. On 21 July 2014, the **Risk and Compliance Committee** received a paper that summarised the findings and recommendations of Deloitte's Project Zebra. The paper outlined Post Office management's proposed actions concerning testing controls around Balancing Transactions, improvements concerning the FSC documentation processes, and a review of the risk and control framework around the Horizon system.

347. **The Risk and Compliance Committee** was invited to support the proposed actions. However, as with other documents in this statement, I have reviewed this document in isolation and have been unable to establish through the review of further documents whether the RCC did ultimately do so.[381]

348. I have had sight of an internal Post Office '**CIO Risk Log**'[382] from April 2016 which noted that: *"There is a risk that unauthorised individuals have access and those who have left the business may also still have access, which will result in potential security violations and consequences to the Post Office business".*

349. A review was subsequently commissioned by Post Office's then Chairman, to be conducted by Jonathan Swift QC and Christopher Knight, which reported in

[381] POL00206524
[382] POL00401633

WITN03680200

February 2016.[383] This referred to Deloitte's reporting in May and June 2014 and noted that: *"Deloitte's Board Briefing highlights two aspects of Horizon which are relevant to this part of the Review and which we found to be more clearly set out than in any other document we have seen on this subject*."

350. It was also stated by Deloitte that, following a review of the technical documentation, the ISAE3402 and verbal discussions with Post Office and Fujitsu it had identified:

a. database access privileges which "*would enable a person to delete a digitally signed basket*" do exist,but are "*restricted to authorised administrators at Fujitsu*".

b. Those privileges "*would enable a person to create or amend a basket and re-sign it with a 'fake' key, detectable if appropriately checked*".

351. Deloitte had not identified specific controls to prevent a person with the appropriate authorisation carrying out the exercise described above in an unauthorised manner.

352. The document went on to state that administrators had the ability to "*delete data from the Audit Store during the seven year period, which was a matter…contrary to POL's understanding…This could allow suitably authorised staff in Fujitsu to delete a sealed set of baskets and replace them with properly sealed baskets, although they would have to fake the digital signatures*". When we spoke to Deloitte, they described this functionality as resulting, in essence, from the level of security contained in Horizon being a level down from the maximum.

[383] POL00030452

WITN03680200

353. The document went on to state that:

a. "*We have seen a response from Fujitsu concerning this aspect of Deloitte's investigation, which is based upon a summary of it provided by POL rather than the original Board Briefing itself. Fujitsu appear to accept that Deloitte's interpretation is technically correct, but emphasise the wide range of security measures in the software, hardware and environment which reduce the risk of interference. Fujitsu also, properly, stress that there is no evidence that any such action has occurred and that likelihood of all the security measures being overcome is so small that it does not represent a credible line of further enquiry.*"

b. *"The fact that such activity is possible does not, of course, indicate that it has actually occurred. We find it difficult to see why it would have done so."*

354. Pursuant to their instructions, Jonathan Swift QC and Christopher Knight made two recommendations concerning further investigations into remote access that should be carried out by Post Office. These were, in summary, that: Post Office instruct a suitably qualified party to carry out:

a. a full review of the use of Balancing Transactions throughout the lifetime of the Horizon system, insofar as possible, to independently confirm from Horizon system records the number and circumstances of their use; and

b. a full review of the controls over the use and capability of authorised Fujitsu personnel to create, amend or delete baskets within a sealed

WITN03680200

Audit Store throughout the lifetime of the Horizon system, insofar as possible.

355. I have not been able to establish, based on my review of documentation for the purposes of preparing this statement, if these recommendations were carried out.

356. It is my understanding though that, thereafter, in 2016, Deloitte circulated a preliminary '**Project Bramble**' report. This observed that certain privileged Fujitsu users were able to add, amend or delete transactions entered by branch staff on Horizon outside the specific functionality of the system were considered to be particular material.

357. Deloitte also circulated a draft "Project Sparrow" report for discussion in July 2016[384] concerning the use of balancing transactions. Amongst other matters, the report noted in respect of "superusers" that: *"At various layers of the Horizon infrastructure there exist accounts with privileged access rights which could be used to modify or insert data relevant to transactions at branches should they not be adequately controlled. For example, a superuser account on the Oracle DB forming the nucleus of the Branch Database could insert transactions directly onto the backend (effectively Balancing Transactions are a specialised 'legitimised' way of using such Oracle access).*"

358. It is my understanding that Deloitte prepared a draft third version of the Bramble report on 27 July 2016 and subsequently in October 2016[385].

[384] POL00029984
[385] POL00400064; POL00400125.

WITN03680200

Thereafter, between October and December 2017, Deloitte produced further drafts of the Bramble report[386], which stated (amongst other matters) that:

a. *"A limited number of authorised Fujitsu personnel (19 at the Operating System layer and 26 at the database layer, at the time of testing – May 2016) have sufficient privileges to theoretically add / delete / change data in the BRDB (Privileged Users). However, see paragraph 1.4.2.10 below regarding the segregation of access conditions. These users may also have access to other systems, such as the Audit Store, however in the current circumstances access to the BRDB is the most important as it is the BRDB that generates the branch accounts and is the source of the data ultimately used to hold Postmasters liable for shortfalls*.

b. *Post Office personnel do not have this Privileged User access and Fujitsu and Post Office have asserted that they have never had such access, however there is no historic record of all the Privileged Users that there have ever been, so this cannot be verified*."

359. EY, in their capacity as "Independent Service Auditor", contained in the '**Description of Fujitsu's System of IT Infrastructure Services**' for the period 1 April 2017 to 31 December 2017[387], stated (amongst other matters) that: "*...the controls related to the control objectives stated in the Description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period 1 April 2017 to 31 December 2017 and if POL applied the complementary user entity controls contemplated in the design of Fujitsu's controls throughout the*

[386] POL00401550; POL00400287
[387] POL00401634

WITN03680200

period 1 April 2017 to 31 December 2017 .c. the controls tested, which, together with the complementary user entity controls referred to in the scope paragraph of this report if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period 1 April 2017 to 31 December 2017."

360. A further draft Bramble report wasprepared by Deloitte in February 2018[388]. In relation to Horizon Online and remote access, the report found:

a. *"Fujitsu (but not Post Office) has the ability to add, amend or delete transactions entered by branch staff on Horizon via Privileged Users outside of specific functionality of the Horizon application.*"

b. "*A limited number of authorised Fujitsu personnel (19 at the Operating System layer and 26 at the database layer at the time of testing - May 2016) have sufficient privileges to theoretically add / delete / change data in the BRDB ("Privileged Users").*"

c. *"Post Office personnel do not have this Privileged User access and Fujitsu and Post Office have asserted that they have never had such access, however there is no historic record of all the Privileged Users that there have ever been, so this cannot be verified*."

d. *"Changes to a branch's transaction data in the BRDB by Privileged Users would be visible to branch staff. The amended transaction would show up in transaction reports produced in branch but would not be flagged as a change by a Privileged User and to the best of our*

[388] POL00253246

WITN03680200

knowledge would appear like a normal transaction generated in branch (although see paragraph 1.4.2.14 below around database logging of the actions of Privileged Users)."

e. *"We would expect a system such as Horizon to have this type of Privileged User access as it will be used to undertake maintenance on the system or to implement updates. Such access comes with a risk of it being misused, either by accident or maliciously. It is impossible to eliminate this risk entirely (within Horizon or any other IT system) and so systems generally have controls over the use of privileged access so as to reduce the risk or misuse or to make it detectable."*

f. *"A key control in Horizon is the segregation of access permissions between Privileged Users who can access the BRDB and those users who may access the Key Management Server (KMS). The KMS holds the digital keys that underpin the controls listed in paragraph 1.4.2.2. Segregation of Privileged Users from KMS users means that a Privileged User cannot get around the controls in paragraph 1.4.2.2 and therefore cannot cover up any changes they make in the BRDB (Controls 1.4.2.2 b, c, d and e are of particular importance). If a proper segregation of duties is in place, any changes by a single Privileged User to the BRDB would be detectable in line with paragraphs 1.4.2.2 b, c, d and e above. This does not eliminate the risk of misuse entirely as there could be a conspiracy between a Privileged user and a KMS user."*

361. It is my understanding that Deloitte was unable to carry out testing of Legacy Horizon (named Riposte) but reached the following views on remote access by carrying out interviews and reviewing technical documentation:

WITN03680200

"(a) On the Riposte system the data was held locally on a Branch Server and then replicated to a cluster of central servers overnight. On HNG-X a key principle is branch data is only held centrally (on the BRDB).

(b) A Cyclic Redundancy Check (CRC) function provided functionality similar to the digital signature in that it provided a checksum capability. A checksum applies a predetermined algorithm to a set of data to produce an output. When transmitted or held with the data the checksum algorithm can be reapplied to validate whether the dataset is complete and accurate. Unlike the digital signature applied by Horizon to Counter transactions, this is not cryptographically secure and technically competent people can generate CRCs simply (i.e. it is at greater risk of tampering).

(c) Once data was received from a branch server by the centralised server farm it would be duplicated to all nodes in the farm (they were four clusters), meaning that challenges in terms of altering the data would likely still exist (as data would now be different between different nodes), causing a data integrity issue which would be likely to generate system errors and be noticed if only one location was updated.

(d) Riposte was a third party provided system, meaning that neither Fujitsu nor Post Office would have been likely to have ready access to the source code of the application. Access to source code is an imperative requirement to being able to change the underlying code or functionality of the application and the fact that Post Office or Fujitsu would have probably had to approach the vendor in order to do so, would inherently lower the risk of malicious changes to the application from

WITN03680200

privileged users (although not necessarily the amendment of transactions data within the system).

(e)The Audit Store technology was largely identical to the instance supporting Horizon HNG-X at the point of adoption (including the audit server).

(f) Fujitsu have stated that due to (b), (c) and (d) above an application would need to be inserted onto a branch server to manipulate transactions prior to them being distributed to the datacentre and that whilst there is a theoretical possibility this could be achieved, it is considered by Fujitsu to be a 'remote possibility'."

362. I have had sight of an agenda and meeting pack that was prepared for a meeting of Post Office's **Audit, Risk and Compliance Committee** in May 2019. In that pack, it appears to have been noted that user access was not being removed on a timely basis, as well as concerns having been expressed by PwC in relation to employees who were no longer working for Post Office still having access to Horizon. [389]

363. I have also reviewed a similar agenda from May 2020 which included an audit report by PwC for the year ended 29 March 2020. The report summarised what were described as key deficiencies in Horizon, which included user access rights not being terminated in a timely basis following the users leaving the Post Office[390].

364. In December 2020, KPMG prepared a draft setting out their findings following an audit report of the Horizon system[391]. Amongst other matters, this audit

[389] POL00401577
[390] POL00401577
[391] POL00031727

WITN03680200

noted that there had been no progress in relation to privilege or elevated access controls within the Horizon environment beyond the basic user enablement and access. It was also stated that Post Office used limited controls around remote access.

Question 3(c) – "In respect of any internal measures identified in relation to point b), please set out the technical expertise of those responsible for monitoring compliance."

365. Due to the passage of time, and an associated lack of document retention and corporate knowledge within the Post Office business, I am unable to assist the Inquiry by comprehensively detailing the technical expertise of those responsible for monitoring compliance through the internal measures that I have described above in response to Question 3(b) of the Rule 9 request.

366. However, my colleagues within Post Office's HR department have been able to locate:

a. some examples of role profiles for those who I understand would, during the 2000-2019 period, have played some role in Post Office's internal monitoring of Fujitsu's compliance with the relevant contractual obligations; and

b. some limited information in relation to the technical qualifications held by particular named individuals who I understand would have played a role in the internal monitoring described above.

367. I have set out below, in a table, the details of the role profiles that I refer to above.

WITN03680200

Role/job title	Technical expertise as referred to in the role profile
IT Contract Manager[392]	An ability to determine contractual and financial exposure, negotiate contracts and the ability to participate in the development of the IT asset management mission, goals and objectives. Ability to understand contract risks and to work with other parts of the organisation in crafting tactics and strategies for risk mitigation.
Solutions Architect[393]	Role includes ensuring adoption of and compliance with Post Office enterprise architecture standards/processes (Architecture Quality Plans, Design Reviews etc) and the delivery of all the required architectural deliverables.
Domain CTO[394]	The Domain CTO is responsible for ensuring that good business outcomes, security and regulatory

[392] POL00401675
[393] POL00401676; POL00401677.
[394] POL00401678

	compliance are embedded within the current and future IT systems and processes of the Business Vertical. This role requires being educated to degree level or equivalent experience and for the role holder to have experience of designing or deploying solutions into multi-channel or omnichannel retail businesses- ideally with a background including one or more of Retail, Financial Services, Telco, Mails or Government services.
Senior Service Manager[395]	The service manager is responsible for ensuring consistent process across vendors, SLA compliance and to undertake service escalations as appropriate. The role requires knowledge of ITIL processes and IT service Management processes and the ability to understand the process to manage

[395] POL00401678

WITN03680200

	risk. ITIL qualifications are listed as a requirement for the role.
Senior Business Analyst[396]	The role responsibilities include ensuring compliance with any specific legislative, regulatory, or contractual requirements. The role requires familiarity with concepts in Agile, Lean and BPR methodologies and frameworks; and Experience with tools such as MS Visio, Excel; and Familiarity with relevant platforms and tools e.g. Jira, Service Now. The role lists the following qualifications sought: BCS Diploma in Business Analysis or other recognised BA qualification (desirable); and LEAN Six Sigma Green or equivalent experience

[396] POL00401679

WITN03680200

Service Delivery Manager (Data Services)[397]	The role holder is responsible for ensuring compliance with any specific legislative, regulatory, or contractual requirements, including all Post Office policies, such as; the key policies and procedures on Confidentiality, Conflict of Interest, Business Continuity, Data Protection and Equal Opportunities. The role requires the following qualification in ITIL Practitioner and Service Operations. In addition, it requires Computer Skills - The administrative side of this role requires sound computer skills – including all aspects of Office 365, SuccessFactors, MS Project, Visio, MDM and Credence.

368. I have also reviewed a document that is entitled "Qualifications for IT Managers" which details the members of the Post Office IT Team (a number of

[397] POL00401680

WITN03680200

which I have referred to above) who held an ITIL[398] certification. An ITIL certification is, a qualification that helps the holder to demonstrate an in-depth knowledge of the IT Service Management lifecycle. It is also my understanding that the Codified Agreement was drafted with the ITIL Framework in mind. It was therefore beneficial for those with responsibility for monitoring and managing the Agreement to have the associated ITIL certification, where possible.

Question 3(d) – "Whether Fujitsu incurred any financial penalties (for the avoidance of doubt, including payments for damages) during the relevant period as a result of non-compliance with the relevant contractual obligations"

369. It is my understanding that Post Office's monitoring of Fujitsu's compliance with the relevant contractual (and wider contractual) obligations as part of the Service Review Structure that I have referred to above was closely linked to the calculation of associated financial penalties. Throughout the 2000-2019 period, it is my understanding that Post Office used 'Service Levels Targets' stipulated in SLAs to measure whether Fujitsu were complying with their obligations pursuant to the contract. Fujitsu were responsible for monitoring these Service Levels and reporting the extent to which they met them using the Service Review Book.

370. If Fujitsu failed to meet the SLT, this represented a failure to meet their contractual obligations. However, if they failed to meet them to a significant enough degree (specified by defined thresholds within certain SLTs) then remedies became available to Post Office.

[398] ITIL is a global framework of best practices for IT service management focused on reducing risk, improving customer relations and supporting IT environments.

WITN03680200

371. Although the remedies and thresholds changed throughout the course of the Codified Agreement, it is my understanding that the liability, remediation and payment structure remained consistent throughout the 2000-2019 period.

Thresholds for Remedies

372. In the **Original Codified Agreement,** the different thresholds through which Post Office could seek remedies for contractual non-compliance were:

a. **The Minimum Acceptable Threshold ('MAT').** Post Office was entitled to the remedies in the given Service Level and Remedies Schedule for the given Service if the MAT was breached.[399] For example, Schedule G10 (which concerns Post Office infrastructure services) stated if Fujitsu breached their HSH obligation to repair 'A Priority' problems or incidents within 12 hours, then liquidated damages would become payable. This is shown in the table of "time to repair" profiles in the table below at paragraph 378. In addition, unless otherwise specified, if Fujitsu failed to reach the MAT for a particular service for three quarterly Service Level Measurement Periods in any 24-month period, Post Office was entitled to terminate the Codified Agreement.[400]

b. In addition, if the level of service provided fell below the Termination Review Threshold ('TRT') then Post Office was also entitled to terminate the Codified Agreement.202 In addition, if the service fell below the TRT, liquidated damages and 'failure damages at large[401]'

[399] Schedule A6, 1999 Codified Agreement
[400] Clause 902.2 – as per Paragraph 4.4, Schedule A6, 1999 Codified Agreement
[401] This means that damages would be determined by a court after the breach rather than in the liquidated form provided for in the Codified Agreement.

would, in that instance, be payable. If Post Office decided not to terminate the agreement, an alternative option was available for the parties to agree a method of rectification.[402]

373. In **Schedule 15 of the 2002 Agreement** and **Schedules B4.4 and C1** of the **Current Contract,** the thresholds were expressed differently as follows:

a. **The Liquidated Damage Threshold ('LDT')** which, if not achieved by Fujitsu, gave rise to the payment of liquidated damages in the same way that they would have been payable in the event of a breach of the MAT in the Original Codified Agreement.

b. **An Additional Remedy Level ('ARL')** was the level of service, below the SLT and (if applicable) the LDT, which, if not achieved by Fujitsu, gave rise to the payment of Post Office's Additional Costs.[403] These Additional Costs would be those that Post Office had incurred as a result of breach of the service level – which could include additional staff costs, help desk services or telephone calls.[404]

374. The remedies that were available for different SLTs were summarised in the CCD *'Service Level Targets for Horizon Services',* which referred to the Service Levels from the Codified Agreement but described them in a more user-friendly manner.[406]

---

[402] Original Codified Agreement, Schedule A6, Paragraph 6.4
[403] 2002 Agreement, Clauses, Paragraph 29.1
[404] 2002 Agreement, Interpretation, 'Post Office Additional Costs'

[406] POL00400777

WITN03680200

375. It is my understanding that not every SLT for a Service Level Sub-Obligation had associated remedies. As a result, it was possible for Fujitsu not to meet a SLT without any financial consequences. By way of example, for the 'Hours of Service' Service Level Sub-Obligation, there were no liquidated damages payable regardless of how far beneath the Service Level Target Fujitsu fell.

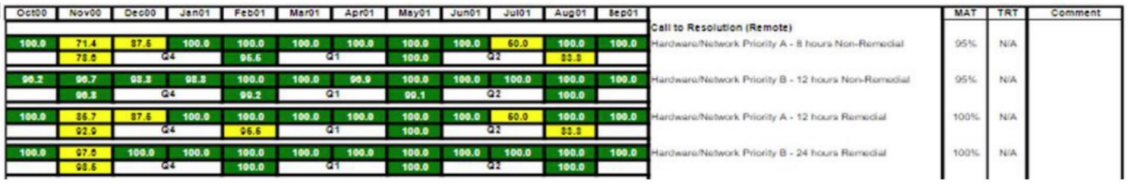
Monitoring of Liquidated Damages and Monitoring of Service Levels

376. The monitoring of liquidated damages was closely linked to the Service Review Process.

377. The Service Review Book contained an annex that detailed which remedies were payable between **Version 1** at the beginning of the term and **Version 2** of the new series issued on 20 February 2008 – after which point this obligation was removed.

378. In the Service Review Book, the performance tables listed which remedy was available for each Service Level Sub-Obligation (as well as using colour coding to reflect the extent to which Fujitsu had met the SLT). As I have explained above in paragraphs 85-90, these are the columns in the right-hand side – which mirror the thresholds for the Original Codified Agreement that I have referred to above. This stated that the MAT would be breached where Fujitsu failed the 12 Hour Time to Repair Obligation for Remote Branches in 95% of cases; which reflects the Liquidated Damages provision in the 1999 Codified Agreement Schedule G10, Paragraph 3.2.2.

WITN03680200



Oct00	Nov00	Dec00	Jan01	Feb01	Mar01	Apr01	May01	Jun01	Jul01	Aug01	Sep01	Call to Resolution (Remote)	MAT	TRT	Comment
100.0	71.4	87.5	100.0	100.0	100.0	100.0	100.0	100.0	60.0	100.0	100.0	Hardware/Network Priority A - 8 hours Non-Remedial	95%	N/A	
	72.0	Q4		96.6	Q1		100.0	Q2		83.3					
90.2	90.7	98.3	98.3	100.0	100.0	99.9	100.0	100.0	100.0	100.0	100.0	Hardware/Network Priority B - 12 hours Non-Remedial	95%	N/A	
	90.8	Q4		99.2	Q1		99.1	Q2		100.0					
100.0	85.7	87.5	100.0	100.0	100.0	100.0	100.0	100.0	60.0	100.0	100.0	Hardware/Network Priority A - 12 hours Remedial	100%	N/A	
	92.0	Q4		96.6	Q1		100.0	Q2		83.3					
100.0	97.5	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	Hardware/Network Priority B - 24 hours Remedial	100%	N/A	
	98.6	Q4		100.0	Q1		100.0	Q2		100.0					

Calculation of Liquidated Damages

379. Each Service Level Sub-Obligation would calculate damages in different ways if the liquidated damages threshold was breached. The method of calculating the liquidated damages due depended on which Service Level had been breached, the scale of the breach (e.g. volume, duration) and the application of any cap on damages. The exact method of calculation would be set out in the relevant schedule of the Codified Agreement.

380. By way of example, **Schedule G10, paragraph 3.2.4** detailed the calculation for the HSH *"Time to Repair"* obligation. When the 12-hour Remedial Timeframe for the "Time to Repair a Remote Priority A incident or problem" was exceeded, the damages payable were then calculated as follows:

a. Downtime cost =

((Seconds of Outlet downtime - (12 * 3600)) * number of automated Counter Positions in Outlet * pence) ;

381. I have reviewed an example of how liquidated damages were calculated in relation to the SLT that related to Branch and Counter Unavailability for the year

WITN03680200

2013/2014[407]. In that instance, no liquidated damages were ultimately deemed payable.

FOR INFORMATION ONLY (as required by CCN1400)
Equivalent Liquidated Damages calculation based on the method in use before the termination of the Service Desk

	Total Additional exclusions after termination of the Service Desk (included in above) (seconds)	

Summary	Failure Type	Seconds of Unavailability per counter	LD Allowance (Seconds) per counter
	Network Wide Failures	0	2808
	Local Failures	0	5940
	Additional exclusions after termination of the Service Desk (included in above)	0	
	Total before additional exclusions after termination of the Service Desk	**0**	**8748**
	LD Seconds of Unavailability	**-8748**	

Liquidated Damages	Year	2013/2014
	LD Payable per hour or part hour	£3.50
	LD Seconds of Unavailability per Counter	0
	LD Hours of Unavailability per Counter	0.00
	Number of Counters	29,761
	LD Total Hours of Unavailability	-
	Total Availability (hours)	6,312,460
	LD Payable	£0.00

Financial Penalties for Failing to Meet Service Levels

382. Throughout all of its versions, the MIS:SD that I have referred to above at paragraph 84[408] stated that if Post Office disagreed with Fujitsu's calculation of liquidated damages this would, at first, be discussed at an Operational Level. Should this fail, it would be escalated to the Senior Management Level (the Horizon Forum (See paragraph 75)) and then the Commercial Level. The Board that sat at the Commercial Level differed across the three Agreements. By way of example:

a. In the **Original Codified Agreement**, under Schedule A04, it was the Contract Steering Group who resolved issues that were no resolved at the Horizon Forum;

[407] FUJ00080297
[414] This defined the contents of the Service Review Book and explained its purpose. It stated it was the "*primary input into the Service Management Forum on performance against SLTs*". It also detailed the other monthly reports that Fujitsu were obliged to provide.

WITN03680200

b. In the **2002 Agreement,** under Schedule 4, it was the Commercial Forum;

c. In the **Current Contract, under Schedule A2**, it was the Commercial Relationship.

383. Across the three Agreements, this was the Board that managed and administrated the Codified Agreement as a whole – and it is my understanding that Board meetings were attended by both party's Contract Managers and Commercial Managers/Directors.

384. Once Post Office and Fujitsu concluded that there had been a failure to meet a Service Level, it is my understanding that Fujitsu was obliged to pay Post Office in accordance with the applicable associated type of remedy (ARL or LD) and the calculation stipulated in the Codified Agreement.

385. Specifically, Schedule 9 of the 2002 Agreement stated that payment would be in the form of Credit Notes (or, at Post Office's discretion, payments of cash) – in accordance with Clause 29, which states that the payment should be within 30 days. Post Office needed to have actively exercised the option to receive liquidated damages otherwise it would be deemed, pursuant to the Codified Agreement, to have elected to receive Service Credits instead.[409] [410] [411]

386. The Service Credits were required to be credited, or liquidated damages paid, within 30 days of receipt of a valid claim made by the Post Office.[412] Any claims

[409] 1999 Codified Agreement, Clause 802.2
[410] In terms of impact, Service Credit would be the same in practice as a Credit Note.
[411] The way in which Service Credits would be credited would normally, as I understand it, be facilitated through deductions from service charges (which are billed monthly).
[412] Clause 802.5, 1999 Codified Agreement

WITN03680200

for liquidated damages and Service Credits were subject to the aggregate liability caps.[413]

387. It is my understanding that these credit notes were issued on a standard form invoice, which detailed the Service Description and amount payable. These invoices also tracked the number of Manual Error Reports throughout the given quarter.[414]

Instances of Liquidated Damages being paid by Fujitsu for breaches of the relevant contractual obligations.

388. It is my understanding, having spoken with colleagues in Post Office's Finance Department, that responsibility for operating Post Office's accounts payable lay with Royal Mail Group until September 2014. Enquiries have been made with Royal Mail Group who no longer hold any documentation associated with that function. Efforts have also been made to contact HCL Technologies, who were the associated software provider for the period up till 2014, but these efforts proved unsuccessful. As a result, I am not able to assist the Inquiry in identifying any instances of liquidated damages being paid by Fujitsu for breaches of the relevant contractual obligations between 2000 and 2014.

389. It is my understanding though, having spoken with colleagues in Post Office's Finance Department, that 96 Credit Notes have been identified for the period between 2014 and 2017. However, it is my understanding that, as the records associated with those Notes were not complete, it is hard to determine exactly what the Credit Notes related to. I have been advised that significant references are made in the associated documentation to rebates being paid to Post Office

[413] Clause 810.2.4, 1999 Codified AgreementClause 32.1, 2002 Agreement
[414] FUJ00234704

WITN03680200

where time, materials or disbursements incurred by Fujitsu pursuant to their contractual obligations were less than expected or the metrics delivered were lower than estimated. As a result, on the limited information that has been provided to me about these Service Credits, it would seem that they were not examples of liquidated damages being payable by Fujitsu as a result of a breach of the relevant contractual obligations.

390. It is my understanding, having spoken with colleagues who were involved in Contractual management of the Codified Agreement during the period from 2017 onwards, that a credit deemed payable in relation to an SLA or SDT breach would be deducted from the following month's invoice as issued by Fujitsu. A formal credit note would only, as I understand it, be issued at Post Office's specific request.

391. I understand that SLA/SLT credits, if issued, would, from at least 2017 onwards, be recorded in the documents associated with the Monthly Commercial Review Meetings and on the face of any invoices applying the credits. However, I have not been provided with or identified any such documents.

392. It is my understanding that, since 2017, there has only been one instance of Fujitsu being required to pay liquidated damages for an identified breach of the relevant contractual obligations. This occurred when Fujitsu failed to deliver Automated Payment Service data files to the Post Office Data Gateway against the SLT, as detailed further below.

WITN03680200

Description	SLT	Liquidated Damages Formula
Failure to deliver files to PODG by 23:59 of the AP Client Delivery Day, per SLT Calendar Year	<=2(*)	Number of Transactions in the non delivered PODG data file x 1.46p(**)

393. The SLT is based on the number of files non-delivered, the Liquidated Damages calculation is based on the number of transactions. The number of transactions contained within the 238 files non-delivered are 943,239. Following the relevant Schedule, the calculation was (£0.0146 x 1.4328) x 943,239 = £19,731.50.

394. The £19,731.50 was invoiced as a credit to the monthly operating fee invoice, in accordance with the process that I have detailed above.

Question 4 – "Please also address: (a) What, if any, changes or improvements have been made since 17 December 2019 to the present day to the levels of testing, monitoring, compliance and reporting on (i) bugs, errors and defects in the Horizon IT System (ii) other network and system failures and (iii) the impact of such events upon branch accounts; (b) What, if any, changes or improvements have been made to the management, rectification and reporting of bugs, errors and defects in the Horizon IT System since 17 December 2019 to the present day.

WITN03680200

395. In my role as IT Director for Horizon, I am responsible for:

a. managing the Post Office Horizon Leadership Team and working with third party suppliers involved in **Horizon**, which is made up of various sub-teams which focus on different aspects of the Horizon IT System (including Postmaster Experience, Commercial Management, Quality Assurance, Horizon Live Services, Remediation and Change as well as Security, Risk & Investigations).

b. designing and implementing changes following the GLO litigation to ensure that Post Office IT takes steps to resolve issues identified in the Horizon Issues Judgement (HIJ).

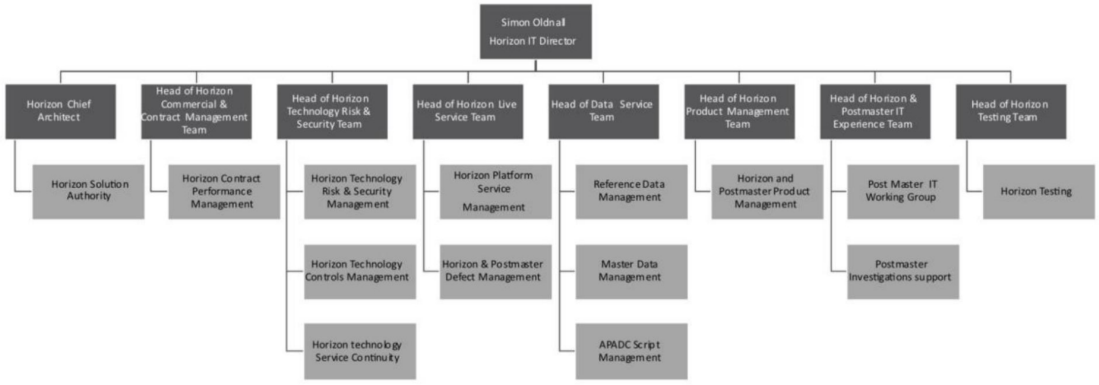
c. Supporting the Post Office Chief Transformation Officer and forming part of the Post Office Technology Leadership Team.

d. In order to support my response to question 4 of the Rule 9 request, I have included the diagram below that illustrates the teams that are responsible for the processes outlined in my statement.

WITN03680200

Post Office Limited - Document Classification: INTERNAL

Horizon IT Team
Functional Lead View



396. The Branch Support Centre (which I will refer to below) is part of the Retail Operations Team (which is not part of the Horizon IT Team and hence, not shown in the diagram above). The IT Service Desk (ITSD) (which I will also refer to below) which is part of Post Office's wider IT function supports Postmasters and wider Post Office staff.

My approach to responding to question 4 of the Rule 9 request

397. In Part 1 of this section of my statement, I have responded to Question 4(a) which asks about changes made since 17 December 2019 to the present day to the levels of testing, monitoring, compliance and reporting on i) BEDS in the Horizon IT system ii) other NSFs and iii) the impact of such events on branch accounts.

398. In Part 1, I have also responded to question 4 (b) and outlined changes or improvements that have been made to the management, rectification and reporting of BEDs in the Horizon IT system since 17 December 2019.

WITN03680200

399. In Part 2, I have responded to question 4c) about changes or improvements that have been made to any internal or external measures to monitor Fujitsu's compliance with the Relevant Contractual Obligations (as defined by the Inquiry in R9(48)) from 17 December 2019 to date.

400. In Part 3, I have responded to question 4d).

Summary

401. The overall performance and status of the Horizon platform is managed by Fujitsu via our agreement for the provision of services from Fujitsu, the scope of these services is detailed in response to question 3(a).

402. In terms of Questions 4(a) & 4(b), by way of high-level summary:

a. In January 2021, Post Office established a Horizon Testing Team of 11 Post Office IT employees who test changes made to the Horizon platform and who are responsible for the testing of all changes made to the system either by Fujitsu or by Post Office itself. Testing will occur either when a change is proposed to the Horizon system or following the identification and remediation of a BED. The Horizon Testing Team have introduced a level of rigour to ensure that BEDs are identified before a change is made to the live system. Any BED detected during testing follows a strict process as outlined below.

b. In 2020/2021, following the HIJ, Post Office implemented AppDynamics which is a system manufactured by AppDynamics Inc that is independent of Horizon itself and provides automated monitoring &

WITN03680200

alerting capabilities that Post Office did not previously have to monitor the performance of the Horizon system.

c. If a BED is detected in the live Horizon system (which is the system in operation), it is reported into the ITSD. Reports can be made by a Postmaster, members of their team or other Horizon users such as a Branch Manager conducting a visit. The ITSD is managed by analysts working with various sets of guidance and knowledge documents. The analysts have a set of knowledge-based articles ("**KBAs"**) which is a bulletin of things they need to know. For example, if there is a known BED within Horizon, it will have been the subject of a KBA that the ITSD analysts can refer to in the event that a problem associated with that BED is raised with them. The BED would then be managed through the Defect Management process (which is described further below) which is operated by the Horizon Live Service Team. An investigation is conducted by this team, this investigation is managed and monitored by the Branch Technology Defects Lead.

d. The network that the Horizon system uses to communicate with Post Office branches was managed by Fujitsu at the outset of the Horizon service. However, on 21 May 2015, Post Office entered into a contract with Verizon to take on this management and review function. As a result, any network failures from 2013 to date would be picked up through Verizon. However, on an operational level AppDynamics (as described above) also ensures visibility of network system failures.

WITN03680200

e. The impact of any BEDs or system failures on branch accounts would be identified and managed through the Defect Management Process which I detail further below.

403. As stated above, I joined Post Office in September 2020. Before this date, I am not aware of any coordinated effort to systematically implement a series of improvements or changes in relation to the areas covered in this question.

The Horizon Issues Remediation Programme

404. Following the Horizon Issues Judgment **("HIJ")**, Common Issues Judgment and Hamilton judgments, Post Office embarked on a series of reviews, the purpose of which was to identify what improvements were needed across the Post Office business in order to remediate and improve on the matters set out in the judgments.

405. As a result of the analysis carried out by Post Office following those reviews, a programme of activity to thematically address all 15 of the findings from the HIJ was instigated (the "Horizon Issues Remediation Programme" ("t**he "Programme**")). For ease of reference, I have detailed each of those 15 findings below:

HIJ number	Detail
1	Defects caused apparent or alleged discrepancies or shortfalls relating to sub- postmasters branch accounts or transactions.

WITN03680200

2	Sub- postmasters were not informed about identified defects. Some defects were not identified by automatic system check and as a result, lay undiscovered for years.
3	Legacy Horizon and HNG-X were not remotely robust, as identified by the number of defects found.
4	Data errors, arising from data entry, transfer or processing in both legacy Horizon and HNG-X led to financial discrepancies. Errors in reference data, and 3rd party data contributed to discrepancies in branch accounts.
5	Transaction data reconciliation with 3rd party data leading to manual corrective fixes and transactional corrections.
6	Legacy Horizon and HNG-X measures and controls did not prevent, identify or report or reduce a) data entry errors b) data packet or system level errors c) software coding errors or bugs d) transmission, replication and storage of transactional record data errors e) data stored in the central data centre was not an accurate record of transactions on branch terminal.

WITN03680200

7	Remote access by Post Office and 3rd parties.
8	Availability of information to Post Office and reliance on 3rd parties.
9	Sub postmaster access to information and transparency over the Investigations process.
10	Fujitsu access to and editing transactions / branch accounts for Sub Postmasters.
11	Permissions Controls upon the use of the remote access facility were considered inadequate.
12	How often was the remote and privileged access facility used by Post Office and Fujitsu.
13	Appsup privileged access rights were very wide and had the potential to affect the reliability of sub postmaster branch accounts.
14	Ability for sub postmaster to dispute a discrepancy via Horizon.

WITN03680200

15	Over 100,000 Transaction Corrections issued since 2006; Post Office does not have comprehensive records on how many have been challenged. TCs used to correct branch accounts with no opportunity to challenge.

406. Post Office identified 5 thematic categories from the 15 findings of the HIJ that I have detailed above:

a. Management of Horizon Defects

b. Management of Core Horizon Data (incl. Reference and Third-Party)

c. Management of Privileged and Remote Access to Branch Accounts

d. Management of Discrepancies and Shortfalls

e. Reliance on Fujitsu to Identify Defects and Causes of Shortfalls in Branch Account[415]

407. The first stage of the Programme was a diagnostic activity to identify the current processes in place for various aspects of managing the Horizon platform, this included the management, rectification and reporting of BEDS, the approach to testing the Horizon IT system, as well as the overall governance measures that were in place for the management of the Fujitsu

[415] POL00337672: 05.01_POL_GE_Horizon Issues Judgment (HIJ) Phase 3 update 220124 (1).docx POL00337701: Horizon Issues Remediation Programme - HIJ Progress & Update December 2023 (1).pptx

WITN03680200

contract. The subsequent programme phases have implemented a series of improvements and changes as detailed below.

Improvements to Testing of the Horizon system

408. The testing of Horizon by Post Office has been executed in a number of ways over the lifetime of the system. Between September 2013 and April 2021 this was executed on Post Office's behalf by Atos IT Services UK Limited ("ATOS"). Further details about this are provided as part of my statement responding to question 3 of the Rule 9 request.

409. In January 2021, Post Office began to establish an internal Horizon testing capability (which was the Horizon Testing Team I have described above) and in April 2021, following the creation of that team, the ATOS test resources were transferred back to Post Office, supplementing the test capability. Testing takes place every time there is a proposed change to Horizon to check the functionality is operating as expected and to ensure that the impact of the change does not adversely affect other parts of the system. A change to the system may be required in order to implement new or updated functionality for the Horizon system or where a BED has resulted in a need to change existing functionality.

410. During the course of testing, the Horizon Testing Team's objective is to identify areas of functionality where the system is not working as expected or the system does not meet the requirements which are set out by Post Office when it has identified that new or amended functionality is required. The aim is to ensure the number of BEDs identified gradually reduces as testing is performed. It will never be possible to completely eradicate BEDs from an IT

WITN03680200

system, but the purpose of the Horizon Testing Team's work is to endeavour to reduce the number of BEDs, once identified, in accordance with industry good practice and the defect thresholds set by Post Office that I will discuss further below.

411. This helps to ensure that any proposed changes to the Horizon system have to pass a series of review points before ultimately being released to the live system.

412. The testing work that I have described above is now standard operational practice for Post Office's Horizon IT Team and is aligned to normal industry practice for the management of change within systems that are akin to Horizon. In addition to the testing work that I have described above, a further improvement in testing have been implemented, which include:

a. Embedding consistent processes for the categorisation of BEDS.
b. The setting of threshold limits for BEDS, dependant on their impact and severity (see below).
c. Implementation of supporting systems using industry standards and tools such as Jira (which I describe further below) for the recording of testing activity to ensure transparency and reportability of testing outcomes.

Testing: Embedding Consistent Processes to Identify & Categorise Horizon BEDs

413. A common set of BED definitions has been established to help ensure consistent terminology is used to identify system BEDs going forwards which

WITN03680200

describes the impact of the BED in question. BEDs are categorised by both severity and business impact, as shown in the tables below.

Severity: Extent of impact a BED has on the development or operation on a component or system

Defect Type	Definition
Urgent	The BED would cause business processes or operations to halt or mean Post Office are not compliant or meeting legislation and therefore requires an urgent fix, ideally in the next release.
High	The BED would have noticeable impact to the business, even with workarounds. It can be fixed in upcoming releases; however, a resolution needs to be included within the release.
Medium	BED has minor impact to day-to-day business processes and operations. The BED can be resolved after the current release.
Low	Negligible impact to the business, considered a 'want' more than a 'need' for business process and operations. The BED can be fixed if there is time.

Business Priority: How important business deem fixing a BED in terms of process, system, compliance or legislative impact.

WITN03680200

Defect Type	Description
Blocker	The BED is preventing essential functionality or critical data from executing. There is no workaround for this issue and the solution cannot be implemented completely with the issue unresolved.
Critical	The BED is preventing essential functionality or major data from executing. However, there are processes by which the issue can be worked around.
Major	The BED affects major functionality or non-critical data. There are practical and usable workarounds that can be temporally implement, or the functionality is considered non-essential to the business proposition.
Minor	A minor aspect of the solution is not functioning correctly. There are clear workarounds that will allow the user to easily navigate the system or the functionality is not essential to the business proposition.
Trivial	The error is worthy of note but has no impact on the successful implementation of the solution.

414. This standardisation of terms further enables Post Office to identify the impact on branch accounts. BEDs with the potential to impact on branch accounts would be categorised as urgent and/or high severity and as a blocker and/or

WITN03680200

being of critical priority to be addressed. These would be addressed as a priority over other BEDs that may be identified. For example, a BED classed as Urgent and Critical would be addressed as a priority over a BED classed as Urgent and Major. The time taken to fix any BED depends on the nature of the issue, the associated technical complexity and the delivery mechanism for remediating the defect (i.e. fix and release).

Testing: Setting the Thresholds for BEDs

415. The setting of BED thresholds is normal practice in the delivery and quality assurance of any technology platform. Thresholds are typically set in line with the quality expectations and risk appetite of the organisation utilising technology. BED thresholds that would typically reflect that every system is likely to encounter BEDs over the course of its lifespan either at the point of initial implementation or as a result of changes to the platform being made over time.

416. In 2022, the work that Post Office undertook as part of the Remediation Programme, including the review of the approach to testing was completed. One of the outputs of this review was the creation of a Post Office[416]Quality Assurance Test Strategy. The strategy was created for use by Post Office project delivery teams, external partners (such as Morrisons and DPD and Evri delivery providers), third-party suppliers (such as Fujitsu or Accenture), and internal Post Office business stakeholders (such as the Retail Operations

[416] POL00337565: D.09.19_POLQAStrategy_V1.0 -Copy

WITN03680200

Team), as a guide of the quality assurance and testing activities at Post Office. The objectives of the document were to:

a. Ensure that there is a collective understanding of the test activities, terms and responsibilities across Post Office.

b. Provide details to key Post Office business stakeholders of Post Office's test strategy (per programme or project) which will provide confidence to the Post Office business. The purpose of this was to put in place a robust process when Horizon changes are deployed into the production environment.

c. Obtain sign-off from key Post Office business stakeholders that the testing approach/plan is achievable, and responsibilities of testing activities are understood.

417. As part of the outcome of this work, Post Office recognised the need for a consistent and common list of thresholds for BEDs. This list was required to ensure that following a risk analysis to identify the potential severity and impact of identified BEDs, a consistent and objective approach was adopted to setting limits on the volume of BEDs that would be within the specified tolerances (as defined in the Quality Assurance Test Strategy referred to above) at each stage of the process.

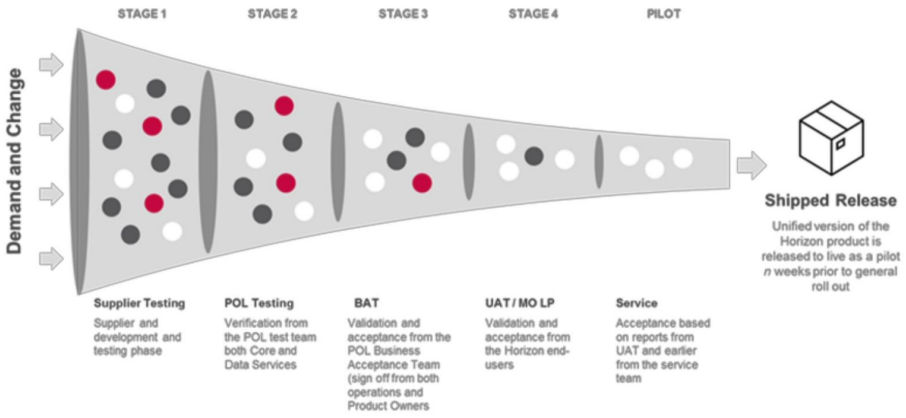
418. This methodology now forms part of the Post Office Quality Assurance Test Strategy which all projects across Post Office are encouraged, pursuant to Post Office's Change Excellence Framework, to follow when conducting testing.

WITN03680200

419. Should a change not demonstrate that it can meet the specified thresholds, it will not be implemented within the live platform so as to maintain the overall integrity the system.

420. Where a change has not been implemented in this way, or if testing has separately led to the identification of BEDs, further testing will then be carried out until such time as the change can demonstrate it does meet the requisite thresholds.

421. As a change progresses through testing, the BED thresholds are examined at each stage as illustrated below.



422. This provides Post Office with an objective metric-based confidence in relation to the Horizon solution which has been provided by Fujitsu and a basis for Post Office's Horizon Testing Team to continually review and assess future changes that may be proposed or deployed to Horizon.

423. Once the change has reached the stage where it is to be applied to the live system, the details of any BED that has been assessed as being within the

WITN03680200

specified tolerances of BEDs that can be within a system at any one time is published to Postmasters in the same way as any BED that is identified through the live operation, for example, if a BED were reported by a Postmaster. These BEDs then follow the Defect Management Process that I describe further below.

Testing: Implementation of supporting systems for the recording of testing activity

424. As part of the work that has been carried out since 2022 which I have described above, Post Office has adopted standard systems for the tracking of testing and the recording of any BEDS identified during testing. This ensures BEDs can be managed consistently using one common tool, as opposed to the multiple Excel spreadsheets and disparate processes that were used previously.

425. During the preparation for the testing of any proposed change to the Horizon system, test scripts are created that detail the testing and checks that will be executed at each stage of the testing. The results of the tests are then recorded within the Jira tool that I will describe further below and which can be used in order to track progress, as well as to provide an audit trail of issues identified during testing.

Analysis of Historic BEDs

426. The first stage of the Remediation Programme also examined the status of historic BEDS that were specifically referred to in the HIJ.[417] Detail was

[417] POL00337564: Horizon Review Report v4.2 Final.pdf

WITN03680200

requested from Fujitsu that enabled Post Office to conduct an analysis of these BEDs. This was provided in the form of a report. [418]

427. A series of joint workshops were then held with Fujitsu staff which resulted in a detailed analysis of the status of these BEDs in the current version of Horizon. The analysis determined that:

a. Out of 63 historical KELs, 46 could be closed as the core system and functionality had extensively changed since these occurred, and thus the specific problems that had been experienced could not occur again.

b. Of the remaining 17 KELs, Post Office and Fujitsu determined that 3 had been resolved and 14 required retesting, to validate they no longer existed within the platform.

c. 3 of the 14 remaining KELs which were the subject of reports made by individual Postmasters and had insufficient detailed technical information to determine what caused the issue or what business process they related to. No further action could be taken in respect of these.

d. Testing of the remaining 11 KELs was successfully completed by Post Office confirming these to have been fixed and no longer prevalent in Horizon.

428. The outcome of testing of the remaining 11 KELs is detailed in the Historic KELs Closure Report (which refers to all the KELs described above)[419] and this report has been shared with Postmasters and the Postmaster IT Working Group. This was an initiative through which Post Office sought the opinions of

[418] Exhibit Reference: FSL_04/260. POL00030528.
[419] POL00337673: Historic KELs Closure Report v0.5.docx

WITN03680200

Postmasters in relation to proposed improvements to the Horizon system and to seek their input in relation to areas in which there could be further improvements.

Management, Rectification and reporting Of BEDs

The Defect Management Process

429. As Part of the Remediation Programme work described above, from February 2020 onwards, there have been a number of updates to the process for managing BEDs within Horizon which can be summarised as follows:

a. The process for the capture and reporting of BEDS and other system errors has been enhanced to ensure that all BEDS identified via testing or via a report from a user (such as a Postmaster, a member of their staff or a Branch Manager who might be conducting a visit to a branch) of the Horizon system are logged in the Post Office service management tool **("ServiceNow")**. The purpose of this is to ensure they are visible and the progress towards resolution can be monitored.

b. This monitoring is carried out at a weekly Defect Management Forum. Since January 2021, these meetings have been chaired by Post Office and are attended by representatives from Fujitsu together with internal teams from the Post Office[420]business. At those meetings, every open

[420] The required attendees for these meetings were: Post Office -Branch Resilience Manager, Head of Horizon Live Services, Senior Service Manager IT Retail, Branch Technology Defects Lead, BRT Operations Manager Branch Reconciliation Team and the Head of the Branch Operations Engagement Team. From Fujitsu, the Defect and Quality Manager was in attendance and Service and Technical Management staff were in attendance from all suppliers.

WITN03680200

BED is reviewed for progress, including those that have had a fix identified and are awaiting their scheduled release, those under development and any in respect of which a solution is still being sought. The information that is considered at these meetings will have been captured via ServiceNow but will also have been reported to the meeting separately by the Branch Support Centre **("BSC")** and ITSD (as described further below).

c. An article for publication to Postmasters is created informing all branches of the new BED and this is published on BranchHub within 48 hours of identification. If the BED has the potential for financial impact, Post Office 's legal team are also advised.

430. The Post Office BSC and ITSD are what I would describe as level one support and are the first point of contact into which users can report problems with Horizon. Both BSC and ITSD are notified of all new problems via the Branch Resiliency Manager.

431. Every update to the record created in ServiceNow is timestamped and all actions and minutes are captured against the record, along with all evidence of any email exchanges, closure notes, supplier updates and test validation sign-off.

432. All problems that have been resolved through the Defect Management Process go through a closure approval process which involves consultation with each of the attendees at the Forum described above prior to being closed. There must be approval from each attendee before a resolved problem can be closed.

WITN03680200

433. Post Office measures the success of the Defect Management Process through a series of key performance indicators, such as how quickly branches are advised of problems and how quickly ServiceNow records are raised.

434. A new Executive level report has been introduced and is published monthly to the Post Office Legal team, the Retail Operations Team and senior leaders within the Post Office records.[421]

435. The overall Defect Management Process and the steps taken by Post Office was reviewed by KPMG in June 2021. [422]

436. In the KPMG report following that review, KPMG commented that:

a. *"The Problem Management process area has been a focus area within Post Office over the past 12 months. A detailed process has been implemented along with the relevant roles and responsibilities to deliver the process and is triggered by a Major Incident or escalated incident. Work is proactively underway to continue to drive improvement in the implementation of the process."*

b. *"There is no universally required project management tooling in place, and some projects are managed via spreadsheets and email, whereas other projects are using an implementation of Jira just for the delivery of that project."*

---

421 POL00337594: BIP Monthly Report – Guide.pptx
POL00337571: Branch Impacting Problems Monthly Report -July 2023.pptx
POL00337574: Branch Impacting Problems Monthly Report -August 2023.pptx
POL00337575: Branch Impacting Problems Monthly Report -September 2023.pptx
POL00337590: Horizon Problems Monthly Report -October 2023.pptx
POL00337570: Horizon Problems Monthly Report -June 2023.pptx
POL00337616: Horizon Problems Monthly Report -December 2023.pptx
POL00337618: Horizon Problems Monthly Report -January 2024.pptx

422 POL00337563: Observations and Recommendations Deliverable – Recommendations Summary v1.1.pptx

WITN03680200

c. *"There seems to be no overarching tool in place to facilitate the delivery of a) project change or b) test management, which causes inefficient control and coordination of change management. Similarly, there is no coordination of metrics, MI, and reporting, and so the governance of each project will be different, and more complex, than if there was a prescribed tool which had to be used for project management*."

437. I will address the work that Post Office has undertaken to address these comments from KPMG further below.

438. Other network errors and system failures are also managed pursuant to the Defect Management Process. The process for managing major incidents, which means any event that may be related to a failure in the network or other system issue, is kept under review and the latest version was produced in July 2023.[423] That process sets out the steps to be taken once Post Office becomes aware of a major incident (either through our system monitoring, a report from a supplier or from a branch via the service help desk).

439. Key elements of the major incident process include:

a. Rapid assessment of the event to determine its severity (including the impact on branches and their ability to trade).

b. Triage of the issue and identification of the steps that are required to remediate.

c. Drafting communications to issue to branches/Post Masters in order to ensure that they are aware of the issue.

[423] POL00337591: Major Incident Management SOP Version 1.1 (2).docx

WITN03680200

440. Once the steps detailed above have been completed, the incident will be managed through records created in ServiceNow, which facilitates the clear tracking of the progress of the process and the auditability of the steps taken to address the major incident. If necessary, a record detailing any underlying problem that led to the major incident will be created and linked to that incident. This record will then be reviewed as part of the Defect Management Process, as described above.

Assessing the impact on branches of BEDS and wider system failures on branch accounts

441. In order to understand the impact of a BED or wider system failures on branch accounts, a step was added to the Defect Management Process that requires a meeting to be held within 48 hours of the reporting of a significant type of incident that I have described above (whether a BED or a system problem) which has the potential to impact on branch accounts.

442. This meeting is attended by the relevant supplier for the service areas that Post Office believes have been impacted by the issue (the supplier would primarily be Fujitsu), representatives from the Post Office IT Horizon Operations Team and Retail Operations Team and the National Federation of Sub-Postmasters **("NFSP")** representatives who are invited to build understanding of the issue or incident concerned.

443. The overall aim of this meeting is to consider any initial workarounds or potential resolutions for the issue that has been identified, and to gather enough

WITN03680200

information for investigation and effective communication regarding that issue to take place.

444. Each BED is categorised as either having the potential to have a financial impact to a branch or could lead to a poor experience for a branch. A criticality score is also allocated to help understand the potential impact of the BED, whether that be on operational capabilities or branch functioning. This enables the Horizon IT Operations team to allocate priority and sequence the timing of fixes.

Establishing more robust governance in Horizon BED Tracking & Resolution

445. Post Office has also introduced improved processes to ensure that BEDs, once identified, are tracked and monitored through to resolution.

446. Post Office uses a number of tools to improve its processes in relation to the monitoring and tracking of BEDs and other service failures, in line with industry best practice. This includes:

a. **Service Now** - Post Office utilises the ServiceNow platform for the execution of a number of our IT Service Management processes. ServiceNow is a cloud-based platform that specialises in IT Service Management & Operations. This is the tool through which, as I have described above, all BEDs are logged.

b. **Jira** - A software package designed to support the tracking and management of BEDs throughout the testing process that I have described above. This tool will also contain test artefacts, scripts and test results.

447. Cross-checking does occur between the systems, but this is not currently automated, which means the two systems cannot yet talk directly to each other. Instead, some of the process is automated and some of it requires manual linking up of tickets and progress. Post Office intends to further mature the use of these tools with an ultimate goal of greater levels of automation. This will provide greater opportunities to identify and predict trends in defects and quality management meaning Post Office is better able to monitor the Horizon system and take appropriate action when issues are identified. This work is part of the response to the issues raised in the KPMG report of June 2021 that I refer to above.

448. All BEDs in the live system are now, once identified, logged in ServiceNow. This ensures progress and activity can be tracked and governed by Post Office's Horizon Live Service Team in one central location, which ensures a complete audit trail. The head of the Horizon Live Service Team and anyone else within Post Office who has responsibility for aspects of the ServiceNow monitoring process has access to the system.

449. A common set of definitions are then used in ServiceNow to categorise the status and progress of the defect as efforts are made to try and resolve it, which I have detailed below.

Defect Status	**Description**	**Actions**	**Who's involved**
In Progress	BED is first identified. Work begins to	Post Office Stakeholders invited to extraordinary meeting of BEDs Forum to socialise issue	IT Digital Service Desk

WITN03680200

	define root cause, reach and scope.	with Suppliers actively diagnosing defect root cause	Branch Support Centre Suppliers (internal and external) providing impacted service
Known Error	BED root cause known and understood.	Workarounds, if required, developed and communicated to affected branches and recorded in Service Now Knowledge Article produced or updated for use by the IT helpdesk	Suppliers (internal and external) providing impacted service Branch Technology BEDs Lead Branch Resilience Manager Knowledge Management Team
Pending Change	BED investigation and root cause identification completed	Change and Release processes engaged and change references/release schedules available or planned Testing completed by Test Analyst with all documentation	Test Analyst Problem Manager / Branch Technology BEDs Lead Service Manager

WITN03680200

		reviewed by Problem Manager or Branch Technology BEDs Lead	Release Manager
Pending Closure Acceptance	Change or Release associated to BED delivered and fix live with service users	BED monitored to ensure fix successful, symptoms no longer prevalent no further related incidents are being raised	Service Manager Release Manager Change Management Team
Closed Resolved	BED resolved and all tasks closed,	All Post Office Stakeholders involved in defect sign off it has now been successfully resolved BED formally closed on ServiceNow	Branch Technology BEDs Lead (coordinates stakeholder sign offs)

450. The weekly meetings of the Defect Management Forum play a key role in this improved governance. The Forum's meetings are coordinated by the Branch Technology BEDs Lead, who acts as a single point of contact within Post Office to track, manage and prioritise resolution of a BED that has been identified. This was a new role that was recruited into Post Office's Horizon Live Service Team. This represents another significant and positive change from previous practices which were not managed directly by Post Office. Post Office are now

WITN03680200

engaged at both a strategic management level and at an operational level in the tracking, monitoring and resolution of BEDs.

451. Forum attendees are asked to assess the potential impact of the identified BED by completing a criticality scoring matrix, which I have included below. This helps to provide a clear prioritisation for the BED, and its level of urgency so work to resolve it can be organised accordingly.

Branch Reconciliation Team	Does the BED cause branch accounting issues? What is the financial scale of the impact? What is the volume of Transactional Corrections for this BED? What is the scale of manual intervention required and volume of calls/ escalations received as a result of the BED?
Branch Resilience Team	How many branches are impacted by the BED? Are customers impacted and if so, what are the volumes? What ticket levels have been received?
Legal & Communications Team	Is the BED causing any reputational damage to Post Office? Could this result in either legal proceedings or media attention for Post Office?

WITN03680200

Branch Technology Defect Lead	Are there any Priority 1 or 2 incidents occurring as a result of the BED? Is the BED impacting the delivery or release of other POL projects or initiatives
IT Security Team	Does the BED present a potential system security vulnerability? Does the BED have any data related risks impacts?
Branch IT Architecture	Does the BED have any impact outside of the product area it relates to? Are there any system configuration or scripting issues as a result of the BED?

452. Post Office has also ensured that the following means of communication have been established and remain ongoing across the Post Office business to ensure any potentially impacted stakeholders of BEDs which have been identified are informed and kept up to date with status.

Product	**Purpose**	**Who's involved**
Branch Hub Article	Ensure branches aware of all known BEDs that could affect them	Branch Resilience Manager drafts article with guidance

WITN03680200

	either financially or cause a detrimental impact on how they work. Done within 2 days of the BED being identified.	from Post Office Comms teams Knowledge Management Team publish article on Branch Hub (within 2 day SLA).
Knowledge Article	Ensure branches receive right support when a BED is experienced. Provide workarounds, as appropriate to support branch operations. Where a BED is financially impacting, escalate to relevant teams e.g. Finance, Operations, Done within 2 days of BED being raised.	Branch Resilience Manager/ Knowledge Management team create and publish. IT Helpdesk teams use the Knowledge Articles to support branch operations.
Defect Notification to Post Office Legal Team	Inform Legal team of each BED which has potential to financially impact a branch.	Branch Resilience Manager Post Office Legal Team

WITN03680200

	As and where appropriate, Post Office Finance teams will also be informed.	

A practical example of the improvements to testing implemented by Post Office: Recovery scripts

453. In order to assist the Inquiry in understanding the improvements to Post Office 's testing of the Horizon system in practice, I include, as an example, the approach that has been adopted in relation to the Horizon Recovery Scripts.

454. Recovery scripts provide Horizon with the steps needed to ensure that in the event, for example, of a loss of connectivity or loss of power, the counter is returned to the stage of a transaction that was being progressed prior to the interruption to processing. An example of this would be, when a Postmaster is processing a Forex transaction and there is a loss of connectivity or power. In that instance, as monies may already have been paid by a customer pursuant to the transaction, the purpose of the Recovery Script would be to ensure that the Postmaster's counter, when connectivity is re-established, is returned to the exact point in the transaction that it was at prior to the loss of connectivity.

455. In January 2022, whilst testing a new element of Horizon, the i-movo voucher encashment functionality, which allows branches to use digital vouchers for benefit payments made via the Horizon Counter, the Horizon Testing team identified a problem with the Recovery Script that had been in place. The purpose of that Recovery Script had been to make sure this process worked correctly in the case of a systems communications or power failure. As a result,

WITN03680200

the problem with that Recovery Script could have resulted in the counter failing to return (as in the example of the Forex transaction I have given above) to the exact point in the transaction that occurred prior to the loss of connectivity.

456. Exploratory testing was, therefore, carried out on a number of Recovery Scripts, as a result of which it was determined that it was necessary to make a change to a piece of software called the Branch Access Layer (BAL). The BAL had been developed by Fujitsu to ensure i-movo transactions on the Horizon Counter worked correctly but had yet to be activated. The output from this exploratory testing was reviewed by the Horizon Solution Authority which is the governance forum within Post Office responsible for oversight of Horizon Design Changes.

457. The issue was promptly escalated via the Horizon Defect Management Process with a recommendation to review all Recovery Scripts to identify whether further defects existed. This also included validating any possible associated financial detriments or operational impacts to Postmasters. This was because a number of the scripts supported transactions with a cash value and therefore had the potential to cause discrepancies in branches if they failed to operate as required.

458. It was identified by the Horizon Solution Authority within Post Office that, whilst making the proposed change to the BAL would resolve the immediate issue with the i-movo Recovery Script, it could potentially also lead to scripts used to support other payment transactions on the Horizon Counter for products such as Drop & Go, Smart Metering and MoneyGram being affected, exposing Post Office and Postmasters to similar operational risks. Approximately 53 Recovery Scripts also supported transactions with a cash

WITN03680200

value, so there was the possibility that this issue could result in branch discrepancies and financial detriment if they failed to operate as required.

459. To understand the extent of the issue, the Horizon testing team carried out a sample regression test on 20 scripts. Regression testing is the re-testing of targeted IT system functionality to ensure that any existing functionality has not been impacted by any changes made in or to the functionality. There is a suite of approximately 900 tests that are run during this process.

460. Through analysis of the results of this sample testing, it was determined it was likely that some of the Recovery Scripts had never performed the appropriate recovery actions they were intended to perform. It was agreed therefore that further testing needed to be performed to fully validate this possibility and identify all impacted Recovery Scripts.

461. Whilst initially identifying some 152 Recovery Scripts as being potentially impacted, further analysis confirmed 88 of the scripts to be obsolete and not linked to any extant processes, reducing the number to 64. A script was deemed to be obsolete if it either related to a business process that was no longer used by Post Office or supported the same recovery process as another script already in use.

462. Where multiple scripts were identified to be performing the same recovery steps, it was identified that this was likely to be due to historic changes to business processes or removal of functionality, without the legacy script having been updated or removed.

463. Testing of the remaining 64 Recovery Scripts was carried out by the Horizon Testing team from March to August 2022. This was a particular cycle of testing which, to be executed effectively, needed to simulate loss of connectivity and

WITN03680200

power at appropriate points in the transaction to ensure the script performed as expected. This cycle of testing also now forms part of the overall testing approach for any changes or new functionality that is deployed by Post Office IT in relation to the Horizon system.

464. These steps provided a worked example of how more robust Horizon testing processes enabled the issue with Recovery Scripts to be promptly identified, understood and managed by the Horizon testing team.

Question 4(c): Changes or improvements made to any internal or external measures to monitor Fujitsu's compliance with the Relevant Contractual Obligations since 17 December 2019

465. The HIJ identified concerns with the extent to which Post Office was reliant on Fujitsu for the management of Horizon and that Post Office had limited control and oversight, from a contractual perspective, on the day to day running of the system.

466. As a result, since the HIJ, Post Office 's IT Commercial Team has been leading an initiative to review existing arrangements, from a commercial perspective, that are in place with Fujitsu and third parties. The purpose of this initiative has been to enhance the working relationship and improve the robustness of the oversight of Fujitsu’s engagement and compliance with the contractual obligations, in order to ensure and effectively support the smooth delivery of Horizon operations.

467. The work that has been progressed pursuant to this initiative can be summarised as follows:

WITN03680200

a. Maintaining the Horizon Agreement with Fujitsu in line with the Post Office 's Contract Management Framework which came into force in 2020.[424]

b. Embedding a robust Horizon IT Commercial Governance model to manage and maintain Fujitsu and other third parties which provide Horizon services to Post Office.

c. Working with teams across Horizon IT Services to identify a key set of Policies, Standards and Frameworks summarising the Horizon Services that Post Office provides to Postmasters and colleagues.

468. I have detailed the work carried out pursuant to each of the workstreams detailed at (a)-(c) above below.

The Codified Agreement within Post Office's Contract Management Framework

469. The Codified Agreement outlines the services which Fujitsu are contractually required to provide to Post Office in order to maintain and support the Horizon system.[425] The Codified Agreement is managed in accordance with the principles and standards of the Post Office Contract Management Framework (as referred to above). This Framework sets out a series of internal controls and operational standards that apply to a supplier management lifecycle, as outlined below, which Post Office Contract Managers must adhere to.

[424] POL00337622: Contract-Management-Framework-Final-2021.pdf
[425] The Codified Agreement between Post Office Counters Limited and ICL Pathway Limited dated 28 July 1999. FUJ00000071.

WITN03680200



470. Through effective and consistent management of suppliers (including Fujitsu) pursuant to the Post Office Contract Management Framework Lifecycle, Post Office has sought to ensure more effective contract management by taking the following steps in relation to all contractual suppliers:

a. Ensuring ongoing compliance with contractual provisions (see further below).

b. Effectively delivering contracts at or under the agreed costs and rates and identifying savings and revenue opportunities throughout the contract management process.

c. Efficiently introducing new suppliers via an onboarding process (which, in summary is when a new contractual supplier starts providing services to Post Office) as well as managing the end of a contract through an exit process (when that supplier ceases to supply services to Post Office) to ensure continuation of products or services with a minimum impact on customers. Contract Managers within Post Office are responsible for the creation of an Exit Strategy. All contracts should, as good practice, include an Exit Schedule which should include obligations to produce (and keep updated), by way of example,

WITN03680200

a draft Exit Plan, to assist with the transition of the relevant service to the next provider.

d. Maximising outcomes to Post Office by the ongoing management of contractual performance, reducing the likelihood of disruption to services to the business, contractual disputes, or reputational damage.

Post Office Horizon IT Commercial Governance

471. Previously, the services provided by Fujitsu pursuant to the Codified Agreement were monitored through the contractual governance schedule which is contained within Schedule A2 of the Codified Agreement.[426]

472. However, as part of the Remediation Programme work that I have referred to above, a governance structure now exists, the purpose of which is to maintain and review the Horizon IT Services which Fujitsu provide pursuant to the Codified Agreement. This governance structure in so far as both Post Office and Fujitsu are concerned is continually reviewed by the Horizon Commercial and Contract Management Team to ensure that it is fit for purpose.

473. Prior to the HIJ, there was already in place a series of monthly meetings with Fujitsu ("the Fujitsu meetings") which covered a variety of topics and issues to ensure that Fujitsu were acting in compliance with their obligations pursuant to the Codified Agreement. These meetings included discussions regarding the requirement to maintain continuity of service with Fujitsu whilst New Branch IT

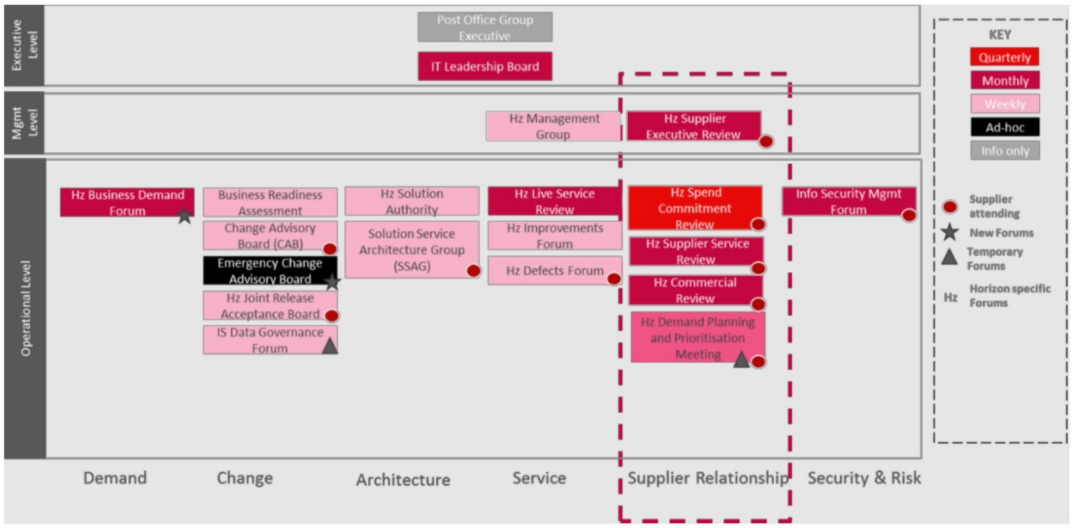
[426] POL00325247: Schedule A2. v14 - Relationship and Governance - FINAL.docx

WITN03680200

– the new system platform which will replace Horizon - came online, reducing any impact to operations during this transitionary period.

474. As part of the Remediation Programme work, Post Office's Horizon IT team scheduled weekly meetings (to supplement the monthly more general contractual meetings described above) to ensure that operational discussions could take place between IT specialists within Post Office and Fujitsu regarding Fujitsu's performance in relation to the relevant contractual obligations and to track Fujitsu's progress on a weekly basis. Matters discussed at these weekly meetings would and continue to be fed into the monthly contractual meetings.

475. I have included below a table that shows how the management of the Fujitsu contractual relationship sits within the broader Post Office Supplier Relationship Governance Model and the associated meetings that take place.



476. I have detailed below further information regarding the purpose, frequency of and attendees at the Fujitsu meetings.

WITN03680200

Meeting	Purpose	Frequency	Attendees
Horizon Supplier Executive Review	Oversee and manage the supplier relationship against overall Post Office strategic direction. Monitor overall success of the relationship with the supplier to foster a collaborative working relationship. Address any operational escalations on supplier in order to resolve in a timely manner.	Monthly	GLO/Horizon IT Director (Chair) Post Office Chief Information Officer Post Office Service Management/ Enterprise IT Director Post Office IT Cloud Services Director Post Office Chief Information Security Officer
Horizon Spend Commitment Review (the meetings associated with this review	Ensure financial commitments are being met and Finance is aligned and aware of any shortfalls or new charges. Review the actual, forecast and committed spend to ensure spend is categorised correctly	Quarterly	Fujitsu Financial Manager (Chair) Post Office Head of Horizon Commercial & Contract Post Office IT Finance (Opex & Capex)

WITN03680200

ceased when the committed spend level was met)			Fujitsu Client Delivery Manager Fujitsu Senior Commercial Manager
Horizon Supplier Service Review (Fujitsu)	Review service availability, utilisation, system performance, capacity. Review and resolve operational services problems being managed by supplier. Encourage continuous improvement in the service management environment through pro-active management.	Monthly	Post Office Horizon Service Manager (Chair) Post Office Commercial Manager Fujitsu Supplier Representative(s) Post Office Horizon Senior Service Manager Post Office CSI Manager (optional) Post Office Head of Live Service (optional) Post Office Horizon Security Manager (optional)

WITN03680200

Horizon Commercial Review	Manage commercial risks, issues and disputes and manage all contract changes. Coordinate administration of the Horizon Contractual Agreement	Monthly	Fujitsu Senior Commercial Manager (Chair) Post Office Head of Horizon Commercial & Contract Post Office Horizon Vendor Manager
Horizon Demand Planning and Prioritisation Meeting	Provide Fujitsu with a future Demand pipeline. Manage current Post Office Demand & priorities. Drive improvements to the Demand process	Weekly	Post Office Head of IT Enterprise Demand Management Fujitsu Programme Manager (Demand Lead) Post Office Head of Horizon Commercial & Contract Post Office Horizon Product Manager Fujitsu Delivery Executive

WITN03680200

477. In addition to the Fujitsu meetings that are described above, Post Office's Horizon IT team also identified two additional opportunities to ensure better working and service delivery by Fujitsu. These opportunities were the creation of:

a. A process of Commercial Governance Continual Improvement; and

b. An internal review of Horizon Service Frameworks, Policies and Standards.

Commercial Governance Continual Improvement

478. As I have detailed above, the weekly Defects Management Forum has been an important governance mechanism which has assisted in raising awareness of BEDs with Fujitsu and Post Office stakeholder groups and ensure all open BEDs are managed and resolved.

479. From a commercial governance perspective, the Horizon Live Services Team (in its capacity as part of the Defect Management Process that I have described above) worked closely with the Horizon IT Commercial & Contract Management team to review the terms of reference of the weekly Forum meeting. This ensured Fujitsu understood the changes to ways of working and the associated impact on BED management but that control in relation to the associated process remained, as I have described above, within Post Office.

Post Office internal review of Horizon Services Frameworks, Policies and Standards

WITN03680200

480. In February 2022, Post Office 's Horizon Commercial & Contract Management Team conducted an internal review of the frameworks, policies and standards in place across each of the Horizon IT service areas within Post Office. This exercise consisted of the following work strands:

a. Compiling a list of frameworks and policies across Post Office Horizon IT on how each of the teams operate, their purpose and objectives[427].

b. Identifying a key set of standards summarising the Horizon Services that Post Office provides to postmasters and colleagues.

c. Reviewing the processes and tools that Horizon IT teams use internally, as well as those which are delivered by Fujitsu to manage the smooth running of Horizon operations.

481. A large volume of documents was reviewed to develop one consistent source of information for the Framework Policies and Standards underpinning Fujitsu's delivery of Horizon IT services to Post Office.[428] This work was conducted in

[427] POL-BSFF-0190573: Documentation Map - All Horizon IT depts (frameworks, policies, standards and processes).xlsx
[428] POL00337642: Application Architecture Policy v1.1.pdf
POL00337649: ARC030 Horizon Solution Architecture Outline.pdf
POL00337643: Architecture & Design Principles.pdf
POL00337562: Architecture Governance v1.0.pptx
POL00337615: ARCSOLARC0001_v8.2 - Horizon Solution Architecture Outline.doc
POL00337647: D10-014 - PROVE PLAN Horizon Improvements Programme v1.0.pdf
POL00337648: EPIC Review process (Horizon System Improvement Process Guide).pdf
POL00337646: POL Architecture Governance v3.pdf
POL00337645: Post Office API Naming v0.2.pdf
POL00337644: Post Office Microservices Principles v1.0.pdf
POL00337627: Contract Approval Process.pdf
POL00337669: Contract Breaches process Oct 2020 (003).pdf
POL00337664: Contract conformance process.pdf
POL00337663: Contract Handover Form_V2.0_210111.pdf
POL00337665: Contract Interpretation v1 20th March 2018.pdf
POL00337626: Contract Approval Process Quick Reference Guide Feb 2021.pdf
POL00337622: Contract-Management-Framework-Final-2021.pdf
POL00337622: CVM RACI August 2020 v7.pdf

WITN03680200

order to promote more consistent ways of working and understanding of roles across operational teams within Post Office and Fujitsu, how tasks are performed, and risks are managed in line with best practice governance.

PART 3

Question 4(d)(i): The current arrangements within Post Office for monitoring Fujitsu's compliance with the Relevant Contractual Obligations (including the level of technical expertise within the Post Office relevant to monitoring compliance)

POL00337667: Exit Monitoring Plan 170918.pdf
POL00337666: Exit Strategy & Planning_180416.pdf
POL00337624: IT Supplier Tiering Pack Review -April 2021.pdf
POL00337623: Obligations Management V1 250820.pdf
POL00337668: Post Office High level IT Supplier Governance v1.1 Nov 2020.pdf
POL00337628: Strategic IT Supplier Management Team Governance and Operating Model.pdf
POL00337625: Vendor Relationship Mapping Instructions.pdf
POL00337633: Benefits Management.pdf
POL00337637: Change Control and Risk Process.pdf
POL00337633: Change Excellence Framework.pdf
POL00337634: Finance Process.pdf
POL00337640: Lessons Learned Process.pdf
POL00337630: Postmaster Engagement Process.pdf
POL00337641: Processes Standard.pdf
POL00337635: Project Tasks Process.pdf
POL00337638: Resource Management Process.pdf
POL00337631: Stakeholder Gating Process.pdf
POL00337636: Status Reporting Process.pdf
POL00337639: Timecard process.pdf
POL00337632: Tolerance Process.pdf
POL00362905: Acceptable Use Standard v2.2.pdf
POL00362906: Access Control Standard 3.2.pdf
POL00362907: Asset Management Standard 2.2.pdf
POL00362908: BYOD Standard v3.3.pdf
POL00362894: Cyber and Information Security Policy 3.1.pdf
POL00362909: Cyber and Information Security Standard 2.2.pdf
POL00362761: Document Retention and Disposal Policy v1.2 .pdf
POL00362910: Encryption Standard 3.2.pdf
POL00362911: Information Classification Standard 2.2.pdf
POL00362912: Logging and Monitoring Standard v2.2.pdf
POL00362913: Network Security Guideline v2.2.pdf
POL00362914: Patch Management Standard v1.3.pdf
POL00362919: PCI DSS Compliance Guideline v2.9.pdf

WITN03680200

482. Where arrangements or processes that I have described above as having been introduced from 2019 onwards remain in force within Post Office, I have made that clear.

483. However, in addition to those arrangements or processes, additional monitoring of Fujitsu's compliance with the Relevant Contractual Obligations (as defined in Rule 9(48)) has and continues to be achieved through Post Office's Horizon Solution Authority (which I have described briefly above). This acts as an important check and balance through which all proposed changes to Horizon must be successfully approved before any changes are progressed. The members of the Horizon Solution Authority team within Post Office who are responsible for monitoring Fujitsu's compliance hold a variety of technical IT qualifications which are set out in detail in documentation associated with an internal audit that was carried out of Post Office IT staff's qualifications[429].

Question 4)d)ii) The management, rectification and reporting of bugs, errors and defects in the Horizon IT system

[429] POL00362915: Penetration Testing and Vulnerability Scanning Standard v1.3.pdf
POL00362916: Remote Access Standard 1.2.pdf
POL00362828: SDLC Guideline v2.0.pdf
POL00362917: Secure Configuration Guideline v2.2.pdf
POL00362829: Supplier Code of Conduct.url
POL00362918: Vulnerability Standard 1.4.pdf
POL00337657: Attachment 1 -EUC Service Specification Document (MASTER) v8.2.pdf
POL00337572: Change Management Process V3.1.docx
POL00337596: Defects Management Process.pdf
POL00337652: Horizon Data Change Process Overview.pdf
POL00337654: Horizon Release Management -Summary Presentation.pdf
POL00337651: Horizon Support Approval Process v1.3.pdf
POL00337561: IT Change Management Policy v1.0.docx
POL00337656: POL -BCR - HNGA Release and Compliance Baselines -V0-21.pdf
POL00337650: POL Programme Test Strategy v0.4.pdf
POL00337662: Post Office Operational Working Agreement v2 Template.pdf
POL00337576: Problem Management Process Summary V0.1 PS DRAFT.pdf

WITN03680200

484. I have described above in answer to Question 4(d)(i), how the process for the management, rectification and reporting of BEDs in Horizon has been reviewed and revised and how it currently operates so as to ensure that it effectively monitors Fujitsu's performance in relation to the relevant contractual obligations and the existence and requirement to rectify BEDs that may be identified.

Question 4)d)iii) The use of access rights and privileges by Fujitsu employees to remedy errors in transaction data and branch accounts

485. The improvement of Horizon security processes and protocols has been a key area of focus for the Horizon Issues Remediation Programme. This work has been progressed through improvements in the following areas:

a. **Horizon Data Centre Security Reporting & Reviews** - This is an ongoing monitoring process of the physical and technical measures in place to maintain security in Horizon Data Centres.

b. **Horizon Global & SMART ID Account Reviews** - These are reviews of the allocation of access to Horizon provided via Global and SMART IDs to ensure that access is appropriate and remains relevant to and necessary for the roles of the individuals who have been granted that access.

c. **Cloud Security** – This ensures that non-physical Post Office data centres are protected with the same levels of security as physical data centres.

d. External Independent Benchmarking, including Horizon Security Penetration Testing & Horizon Security Audit - Both of these processes are the responsibility of an external supplier outside of Post Office and

WITN03680200

Fujitsu called Nettitude. Nettitude provide reporting to Post Office to address the points detailed above.[430]

486. The overall aim of this work has been to give Post Office and Postmasters more confidence in relation to who is accessing Horizon, when and for what purposes.

Horizon Data Centre Security Reporting & Reviews

487. The following processes have been reviewed and improvements have been implemented that have increased the robustness and transparency of access to the maintenance functions associated with the management of the Horizon platform.

Activity	Frequency	Purpose	How it is used?
Horizon Privileged Account Reporting	Weekly	Provides Post Office details of when a Privileged account is used, which is date stamped. Tied to a unique username so	Post Office can drill down to identify suspicious activity or usage patterns usage to see when Privileged accounts are being used in Horizon.

[430] POL00337655: Release Management.pdf
POL00337653: RM-HM-IT Release Management Process V0.4 -draft.pdf
POL00337660: SD&T High Level Process.pdf
POL00337661: Service Design and Transition Policy v2 5.pdf
POL00337621: Capability Statement.xlsx
POL00337567: Penetration Testing Management Report
POL00337568: Penetration Testing Technical Report

WITN03680200

		can be traced and tracked if required.	
Reporting on Remote access to counters	Weekly	Details when remote connection made to Horizon counter. Date stamped and tied back to a Service Now ticket, including FAD code and command run.	Post Office can identify why and when remote access to Horizon counter is made to establish any common patterns of activity.
Appsup review process	Twice a year	Review between Post Office & Fujitsu of process which governs the use of the Fujitsu Appsup role used when Fujitsu are required to provide diagnostic support and other contractual obligations.	Post Office can use this process to determine the parameters in which Fujitsu use the Appsup role to perform support tasks in Horizon.
Breakglass Reporting	Monthly	Provides details of when the last resort password was used along with the	Post Office can use this report to assess whether Fujitsu users have the right set of privileges.

WITN03680200

		reasoning behind its use.	
Failed logins	Monthly	Shows failed logins by Fujitsu support staff.	Post Office can use this report to identify any potentially suspicious activity by seeing the number of unsuccessful attempts made by Fujitsu to log onto the Horizon counter.
Privilege reduction for Fujitsu access to Horizon counter for support purposes	Go Live scheduled prior to Change Freeze Intention to review on quarterly basis	Implement a 'least Privilege model' for access to Horizon Counter by Fujitsu support staff remotely connecting to counter for support purposes e.g. diagnostics.	Post Office can use this approach to improve governance and reduce risk by removing un-needed privileges of Fujitsu accounts to Horizon Counter.

WITN03680200

Total Privileged accounts usage	Monthly	Provides Post Office with regular view of number of Privileged accounts in use	Post Office can use this report to analyse usage trends of Privileged Accounts by Fujitsu and manage any risks.

488. Whilst carrying out this work, Post Office has also taken the opportunity to initiate additional value add activities. These were not within the original remit of the work carried out pursuant to the Remediation Programme but have assisted in further enhancing the robustness of Horizon.

Fujitsu remote access solution

489. Work is ongoing to upgrade the Fujitsu remote access solution which is a software package called Cygwin, through which Fujitsu can access the Horizon counter within branch in order to maintain elements of the Horizon system. As a first step in this work, a study has been commissioned to determine options for the current End of Service Life (EOSL) component – a key element of the existing remote access solution.

490. Due to the age of the component, it cannot be automatically upgraded to the latest version. The study is therefore assessing how the upgrade can take place whilst keeping the Horizon Counter secure and providing Fujitsu with the minimum level of access that they require to provide continued support.

WITN03680200

491. The remote access solution was upgraded in 2023 to protect against vulnerabilities and further restrict the resources on counter devices that Fujitsu have access to. This product allows Fujitsu users to connect via Secure Shell[431] to the counter device and run scripts which allow the retrieval of log information. This method of connection does not allow a Fujitsu user direct control of the desktop or application within a branch.

492. Any remote access, should it ever need to be required, needs pre-approval from senior Fujitsu management, Post Office's Horizon IT and Retail Operations Teams and also requires the involvement of the relevant Postmaster. Any use of these capabilities, which is extremely rare, is retrospectively analysed by the Post Office Horizon Technology Risk and Security team to ensure that all approval steps were followed.

Horizon Global & SMART ID Account Reviews

493. Post Office needs to ensure, so that it can effectively manage remote access to Horizon, that it has robust processes in place to monitor user accounts. By doing so, Post Office will have assurance that accounts are up to date and being used for the purposes they were intended for. The following initiatives have been delivered within Post Office in support of this requirement:

Activity	Purpose	Benefit

[431] This is a protocol that is used to establish a secure connection to a remote machine over which a user can pass commands.

WITN03680200

Global IDs Recertification (Post Office associated)	Verified all current Post Office Global IDs, with those no longer required de-activated and removed 311 Global IDS reviewed with 61 accounts removed Global IDs are used by Post Office to support Postmaster training and other activities e.g. auditing	Ensure Post Office has an accurate and up to date view of active Global IDs being used on the Horizon Counter and the purposes these are used for to ensure more robust governance
SMART IDs Recertification	Identified and de-activated 40,000 un-used SMART IDS 45,000 SMART IDs currently in use across branch estate with processes set up to regularly review these	Ensure Post Office performs routine Security housekeeping governance by removing dormant accounts which could be used to access the system fraudulently

494. A subsequent review of Global ID Privileges was also initiated to assess which privileges were associated to each of the Global ID Roles. This followed a "least privilege" principle whereby each Global ID user would only be assigned the specific privileges needed to fulfil the duties of their role. The findings and

WITN03680200

outcome of the review were made available in Quarter 1 of the 2023 financial year[432].

495. Regular meetings between Post Office and Fujitsu to review Privileged and remote access management initiatives have also been established. These meetings are a key part of the overall ISMF within Post Office that is attended by representatives from Fujitsu and which I will describe in more detail in my response to question 3 of the Rule 9 request.

Cloud Security

496. There are some further initiatives that have also been instigated within Post Office in an effort to improve the security and access privileges associated with a small amount of Horizon applications which Fujitsu support and have already migrated to the Post Office Cloud, which I have detailed further below. Work has also been done to update documentation around Appsup which is a process that is used by Post Office to ensure any elevated privileges required by Fujitsu to support applications they are responsible for in the Post Office Cloud are approved by Post Office before access is granted. These are as follows:

Activity	Purpose	What did we do?

[432] POL00337699: Global User Review Completed Second Review of 2022.xlsx
POL00337700: Global User Review Completed Second Review of 2023.xlsx

WITN03680200

New Joiners template for Fujitsu user access requests	Ensure robust 'Joiners Mover and Leavers' process in place for Fujitsu staff who require access to applications which sit in Post Office Cloud environment (AWS) for support purposes	New Fujitsu user requests by Fujitsu must raise JIRA ticket and complete the new joiners' template to show which access groups the Fujitsu user needs to be added to Joiners template under review following close of Belfast Exit project to remove access groups no longer relevant
Fujitsu User Recertification	Recertify all current Fujitsu users, ensuring this list is accurate and up to date so that only access is only given to individuals who require this for the purpose of their role	Post Office completed one off exercise with Fujitsu to ensure list of Fujitsu user access accounts was up to date Not all Fujitsu accounts recertified as Post Office could not see all users – resolved through improved regular reporting Further recertification exercise underway following close of Belfast Exit project

Regular Recertification Process	Ensure that there are regular reviews of who from Fujitsu still have access to and still require access to the Post Office Cloud in order to support applications	Post Office initiated monthly review of Fujitsu user accounts to ensure they are up to date For any accounts no longer required, Fujitsu must raise a Jira ticket for Post Office to action this (with support of DXC)

Horizon Security Penetration Testing

497. Further initiatives have also been instigated within Post Office to ensure that Post Office is acting in accordance with wider industry best practice security protocols (that relate to issues such as physical system security) in so far as systems access is concerned. These initiatives were as follows:

Activity	Purpose	Findings
Model Office Testing	Testing of build of live Horizon counter and robustness of Operating system concluded it was not possible to break into the	Strong security overall with good infrastructure configuration confirmed it was not possible to break out from the Post Office Counter Browser Application with data also secure from adverse tampering. Minor improvements highlighted to enhance port security and network access control measures on network switches connecting

WITN03680200

	counter Operating system	counters as well as disabling NetBIOS and other legacy Security protocols
Data Centre Testing	Post Office commissioned an onsite health check of overall internal security infrastructure	Unsupported Operating systems were in use within the Post Office network which could be exploited from a Security perspective Parts of Microsoft Windows infrastructure were vulnerable as patches not applied correctly exposing security of Post Office's internal environment Various areas regarding encryption and unprotected files were identified where improvements could be made.

498. Findings from the Data Centre testing have been taken forward for review by Post Office's Horizon IT team with a focus on ensuring remediation plans are put in place with Fujitsu to address, as a priority, critical and medium level issues that have been identified.

499. As an additional value-add activity, an analysis of the Horizon Counter set up within Post Office Counter Training Offices was commissioned and has been carried out[433] which focused on assessing whether the correct security

[433] As per 16.

WITN03680200

protocols are in place on counter terminals used for training Postmasters and Post Office colleagues, so they are fit for purpose.

Horizon Security Audit

500. An annual independent audit by Ernst and Young is also carried out on Fujitsu operations covering the process and governance surrounding Privileged Access Management.[434]

Statement of Truth

I believe the content of this statement to be true. .

Signature: GRO

Date: 30 April 2024

[434] POL00337569: Fujitsu-Post Office ISAE3402 Report -1 April 2022 to 31 December 2022.pdf

WITN03680200

IN THE POST OFFICE HORIZON IT INQUIRY

Index of Exhibits to the witness statement of Simon Geoffrey Oldnall on behalf of Post Office Limited in response to Rule 9 request 48

Number	Inquiry URN Number	Document description	Control/Production Number
1.	POL00424367	Note on Post Office Limited's response in relation to questions 3(e) and (f) of Rule 9(48) – provided to Inquiry via email on 15 March 2024	POL00424367
2.	POL00393860	Description of Fujitsu's System of IT Infrastructure Services Supporting Post Office Limited's POLSAP and HNG-X Applications, 1 April 2012 to 31 December 2012	POL-BSFF-0220538
3.	POL00424366	Glossary of terms – provided to Inquiry via email on 19 March 2024	POL00424366
4.	POL00399924	Email from Babu Palathoti (Post Office Limited) to Kenneth Garvey (Post Office Limited) and Tom Porter (WBD) attaching Original Codified Agreement and schedules, 17 June 2016	POL-BSFF-0226594
5.	POL00325269	Second Supplemental Agreement, 24 September 1999	POL-BSFF-0163015
6.	POL00324066	Third supplemental agreement between POCL and ICL, 19 January 2000	POL-BSFF-0161812
7.	POL00393858	Original Codified Agreement, Version 1.2, 8 February 2000	POL-BSFF-0220536
8.	POL00028202	Original Codified Agreement, Version 1.3, 14 April 2000	POL-0024684
9.	POL00393914	Original Codified Agreement, Version 1.4, 25 July 2000	POL-BSFF-0220584
10.	POL00043749	Original Codified Agreement, Version 2, 12 January 2001	POL-0040252
11.	POL00337516	Original Codified Agreement, Version 3, 19 September 2001	POL-BSFF-0163728
12.	POL00394103	Original Codified Agreement, Version 4, 25 June 2002	POL-BSFF-0220773
13.	POL00337524	Original Codified Agreement, Version 5, 30 October 2002	POL-BSFF-0163736
14.	POL00393881	ICL Pathway Core System Release Contents Description, 25 June 1999	POL-BSFF-0220551
15.	POL00325101	Original 2002 Agreement, 31 December 2002	POL-BSFF-0162847
16.	POL00324108	2002 Agreement, Version 2, 6 August 2003	POL-BSFF-0161854
17.	POL00324122	2002 Agreement, Version 3, 5 November 2003	POL-BSFF-0161868
18.	POL00324132	2002 Agreement, Version 4, 26 August 2004	POL-BSFF-0161878
19.	POL00324165	2002 Agreement, Version 5, 5 July 2005	POL-BSFF-0161911
20.	POL00324169	2002 Agreement, Version 6, 30 November 2005	POL-BSFF-0161915

WITN03680200

21.	POL00324187	2002 Agreement, Version 7, 15 August 2006	POL-BSFF-0161933
22.	POL00394114	Network Banking Service (NBS) Definition, 4 November 2002	POL-BSFF-0220784
23.	POL00324232	Current Contract, Version 1, 31 August 2006	POL-BSFF-0161978
24.	POL00324248	Current Contract, Version 2, 24 January 2007	POL-BSFF-0161994
25.	POL00324286	Current Contract, Version 3, 6 July 2007	POL-BSFF-0162032
26.	POL00324311	Current Contract, Version 4, 14 April 2008	POL-BSFF-0162057
27.	POL00324320	Current Contract, Version 5, 23 February 2009	POL-BSFF-0162066
28.	POL00324356	Current Contract, Version 6, 7 July 2009	POL-BSFF-0162102
29.	POL00324386	Current Contract, Version 7, 10 May 2010	POL-BSFF-0162132
30.	POL00324419	Current Contract, Version 8, 21 February 2012	POL-BSFF-0162165
31.	POL00324460	Current Contract, Version 9, 13 January 2014	POL-BSFF-0162206
32.	POL00324548	Current Contract, Version 10, 10 September 2015	POL-BSFF-0162294
33.	POL00324703	Current Contract, Version 11, 31 March 2016	POL-BSFF-0162449
34.	POL00324743	Current Contract, Version 12, 13 July 2016	POL-BSFF-0162489
35.	POL00324964	Current Contract, Version 13, (undated)	POL-BSFF-0162710
36.	POL00325303	Current Contract, Version 14, 20 December 2021	POL-BSFF-0163049
37.	POL00399922	Schedule A04 to the Original Codified Agreement - Contract Management	POL-BSFF-0226592
38.	POL00399922	Schedule A04 to the Original Codified Agreement - Contract Management	POL-BSFF-0226592
39.	POL00393888	Discussion paper: POCL/ICL Pathway Joint Meetings, 27 January 2000	POL-BSFF-0220558
40.	POL00393888	Discussion paper: POCL/ICL Pathway Joint Meetings, 27 January 2000	POL-BSFF-0220558
41.	POL00393888	Discussion paper: POCL/ICL Pathway Joint Meetings, 27 January 2000	POL-BSFF-0220558
42.	POL00393890	Letter from Keith Baines (Post Office Limited) to Tony Oppenheim (ICL Pathway) re POCL/ICL Pathway Joint meetings, 28 January 2000	POL-BSFF-0220560
43.	POL00401664	Letter from Colin Lenton-Smith (ICL Pathway) to Keith Baines (Post Office Limited) re CCN 411a - Charges, 27 June 2001	POL-BSFF-0228334
44.	POL00401663	Letter from Keith Baines (Post Office Limited) to Colin Lenton-Smith (ICL Pathway) re Operational Business Change - Products, 10 August 2001	POL-BSFF-0228333
45.	POL00401662	Letter from Colin Lenton-Smith (ICL Pathway) to Keith Baines (Post Office Limited), re Key Refresh - Clause 409, 6 September 2001	POL-BSFF-0228332
46.	POL00401661	Letter from Keith Baines (Post Office Limited) to Colin Lenton-Smith (ICL	POL-BSFF-0228331

WITN03680200

		Pathway) re Key Refresh - Clause 409, 13 September 2001	
47.	POL00401660	Letter from Colin Lenton-Smith (ICL Pathway) to Keith Baines (Post Office Limited) re CR R181, 23 October 2001	POL-BSFF-0228330
48.	POL00401659	Letter from Keith Baines (Post Office Limited) to Colin Lenton-Smith (ICL Pathway) re CCN 889 - Notification of Closure of Post Office Limited HAPS System, 14 December 2001	POL-BSFF-0228329
49.	POL00401658	Email from Colin Lenton-Smith (ICL Pathway) to Keith Baines (Post Office Limited) re Charges for Changes to AP Client take-on and Token Verification Services, 25 April 2003	POL-BSFF-0228328
50.	POL00401657	Email thread between Colin Lenton-Smith (ICL Pathway) and Keith Baines (Post Office Limited) re Charges for Changes to AP Client take-on and Token Verification services, 7 May 2003	POL-BSFF-0228327
51.	POL00401656	Letter from Keith Baines (Post Office Limited) to Colin Lenton-Smith (ICL Pathway) re Disputed invoices, 30 July 2003	POL-BSFF-0228326
52.	POL00401655	Letter from Colin Lenton-Smith (ICL Pathway) to Keith Baines (Post Office Limited) re CCNs 297, 333a & 437 - Disputed Invoices, 8 September 2003	POL-BSFF-0228325
53.	POL00399922	Schedule A04 to the Original Codified Agreement - Contract Management	POL-BSFF-0226592
54.	POL00393957	Service Management: High Level Process Description - Service Improvement, 14 November 2000	POL-BSFF-0220627
55.	POL00393983	Operational Level Agreement between Post Office Network Business Service Management (Outlet Systems Group) and ICL Pathway, 6 December 2000	POL-BSFF-0220653
56.	POL00394054	Operational Level Agreement - Reference Data between Post Office Limited/ICL Pathway, 22 February 2002	POL-BSFF-0220724
57.	POL00394060	Strategy Statement for Operational Level Agreements, 4 September 2001	POL-BSFF-0220730
58.	POL00393987	Service Level Agreement between Internal Account Management and Business Service Management, 23 April 2001	POL-BSFF-0220657
59.	POL00394118	Service Management Service: Service Description, 31 December 2002	POL-BSFF-0220788
60.	POL00393882	Service Management Framework - Definition, 18 August 1999	POL-BSFF-0220552
61.	POL00400131	Service Management Service: Service Description, 30 November 2016	POL-BSFF-0226801
62.	POL00398160	Post Office Limited Incident Management Framework Document v6.8, 15 August 2013	POL-BSFF-0224830
63.	POL00393957	Service Management, High Level Process Description, Service Improvement, 23 November 2000	POL-BSFF-0220627
64.	POL00393957	Service Management, High Level Process Description, Service Improvement, 23 November 2000	POL-BSFF-0220627

WITN03680200

65.	POL00393987	Service Level Agreement between Internal Account Management and Business Service Management, 23 April 2001	POL-BSFF-0220657
66.	POL00393957	Service Management: High Level Process Description - Service Improvement, 23 November 2000	POL-BSFF-0220627
67.	POL00394001	Email from Annette Bentley (Post Office Limited) to PON_BSM_FOCUS re E-Focus - BSM, 19 July 2001	POL-BSFF-0220671
68.	POL00393875	ICL Pathway Customer Service: Customer Service Operations Manual, Version 0.2, 29 June 1998	POL-BSFF-0220545
69.	POL00401640	Definition of Remote and Intermediate Locations, 19 April 2005	POL-BSFF-0228310
70.	POL00393915	Contract Controlled and Referenced Document List, Version 1.4, 2 August 2000	POL-BSFF-0220585
71.	POL00400777	Service Level Targets for Horizon Services, 5 December 2002	POL-BSFF-0227447
72.	POL00393913	ICL Pathway Audit of the Horizon System HelpDesk, Version 1.0, 28 April 2000	POL-BSFF-0220583
73.	POL00394097	End to End Service Report Service Management, 20 May 2002	POL-BSFF-0220767
74.	POL00394098	Email thread between Sue Stewart (Post Office Limited) and Kevin Lenihan (Post Office Limited) re Cross Domain Meeting Framework, 13 June 2002	POL-BSFF-0220768
75.	POL00394064	Post Office Limited Business Service Management Service Review Framework, 4 March 2002	POL-BSFF-0220734
76.	POL00393913	ICL Pathway Audit of the Horizon System HelpDesk, Version 1.0, 28 April 2000	POL-BSFF-0220583
77.	POL00394091	Horizon Service Review Forum Meeting Minutes, 17 February 1999	POL-BSFF-0220761
78.	POL00394015	Email from Sue Stewart (Post Office Limited) to Post Office Limited employees re Meeting Dates, 28 November 2001	POL-BSFF-0220685
79.	POL00394102	Fujitsu Services Pathway Service Review Book, 12 June 2002	POL-BSFF-0220772
80.	POL00395270	Management Information Service: Joint Working Document, 3 October 2007	POL-BSFF-0221940
81.	POL00394060	Strategy Statement for Operational Level Agreements, 4 September 2001	POL-BSFF-0220730
82.	POL00393913	ICL Pathway Audit of the Horizon System HelpDesk, Version 1.0, 28 April 2000	POL-BSFF-0220583
83.	POL00393787	Horizon Programme - Management of the Live Environment Report No. 31 (March 2000), 17 April 2000	POL-BSFF-0220465
84.	POL00393905	POCL Horizon Programme - Management of the Live Environment - Summary Report No 32 (April 2000), 15 May 2000	POL-BSFF-0220575
85.	POL00393795	Horizon Programme - Management of the Live Environment Report No 33 (May 2000), 12 June 2000	POL-BSFF-0220473
86.	POL00393805	Horizon Programme - Management of the Live Environment Report No 33 (June 2000), 17 July 2000	POL-BSFF-0220483
87.	POL00393817	Horizon Programme - Management of the Live Environment Report No 33 (July 2000), 21 August 2000	POL-BSFF-0220495

WITN03680200

88.	POL00393829	Horizon Programme - Management of the Live Environment, Report No 34, (August 2000), 14 September 2000	POL-BSFF-0220507
89.	POL00393949	Horizon Programme - Management of the Live Environment, Report No 35, (September 2000), 16 October 2000	POL-BSFF-0220619
90.	POL00393917	Horizon Programme - Management of the Live Environment, Report No 36, (September 2000), 12 October 2000	POL-BSFF-0220587
91.	POL00393906	Post Office Horizon Programme - Management of the Live Environment Report No 32 (April 2000), 15 May 2000	POL-BSFF-0220576
92.	POL00393904	Email from Danny Corry (Post Office Network) to MOLE Report group email attaching MoLE Report and Management Summary, 15 May 2000	POL-BSFF-0220574
93.	POL00393898	Unit Risk Profile - Post Office Network, 14 February 2000	POL-BSFF-0220568
94.	POL00393900	Post Office Network Performance Summary, 12 May 2000	POL-BSFF-0220570
95.	POL00393874	Joint Testing Agreement between Benefits Agency and Post Office, Version 0.4, 30 January 1998	POL-BSFF-0220544
96.	POL00397327	G031 Drop & Go Requirements Specification, 2 November 2011	POL-BSFF-0223997
97.	POL00397070	Horizon Security Policy, Version 12, 5 April 2007	POL-BSFF-0223740
98.	POL00397087	POca Service Delivery - Security Policy, Version 2.1, 30 July 2009	POL-BSFF-0223757
99.	POL00400363	HNG-X Generic Acceptance Process, Version 1.0, 21 March 2018	POL-BSFF-0227033
100.	POL00397066	SAP Consolidation Project – Project Initiation Document, 2 March 2009	POL-BSFF-0223736
101.	POL00394339	S52 Release Authorisation Board Agenda, 15 March 2004	POL-BSFF-0221009
102.	POL00400280	Email from Philip Moss (Fujitsu) to Post Office Limited, Fujitsu and ATOS recipients re Release Acceptance Meeting/Release Acceptance Board, 4 October 2017	POL-BSFF-0226950
103.	POL00394195	Email from Debbie Richardson (Fujitsu) to Keith Hall (Post Office Limited) and Peter Jones (Royal Mail) re Summary Report and Revised PinICLs, 31 July 2003	POL-BSFF-0220865
104.	POL00394198	ITU System Validation and Integration Weekly Summary Report, 1 August 2003	POL-BSFF-0220868
105.	POL00394294	Email from Debbie Richardson (Fujitsu) to Keith Hall (Post Office Limited), Peter Jones (Royal Mail) and others re PinICLs Agreed for Futures, 3 October 2003	POL-BSFF-0220964
106.	POL00394296	Futures Spreadsheet, 11 September 2003	POL-BSFF-0220966
107.	POL00394310	Internal Post Office Limited email thread re IRF actions, 19 September – 30 November 2003	POL-BSFF-0220980
108.	POL00394322	Email from Peter Jones (Royal Mail) to Torstein Godeseth (Post Office Limited) re Known Problems List, 9 February 2004	POL-BSFF-0220992

WITN03680200

109.	POL00394532	Email from Peter Jones (Royal Mail) to Sukhjinder Kaur (Post Office Limited) re Testing Query, 6 July 2004	POL-BSFF-0221202
110.	POL00394501	Email from Peter Jones (Royal Mail) to Sukhjinder Kaur (Post Office Limited), Ray Jackson (Post Office Limited) and others re FS Incidents, 29 June 2004	POL-BSFF-0221171
111.	POL00394502	Outstanding Peaks from S60, 28 June 2004	POL-BSFF-0221172
112.	POL00394503	Email from Sukhjinder Kaur (Post Office Limited) to Peter Jones (Royal Mail) re S60 Deferred, 29 June 2004	POL-BSFF-0221173
113.	POL00393982	Problem Management Operational Review Forum Terms of Reference, Version 1, 19 March 2001	POL-BSFF-0220652
114.	POL00178059	Email from Wendell Jones (Post Office Limited) to Problem Co-Ordinators re PC Meeting, 13 November 2001	POL-BSFF-0016122
115.	POL00178060	Problem Coordinator Meeting Agenda, 16 November 2001	POL-BSFF-0016123
116.	POL00178061	Problem Table, 13 November 2001	POL-BSFF-0016124
117.	POL00178062	Problem Management, Status Report, October 2001	POL-BSFF-0016125
118.	POL00178066	Business Service Management, Problem Coordinator Matrix, 13 November 2001	POL-BSFF-0016129
119.	POL00178065	Problem Coordinators Meeting Note, 12 October 2001	POL-BSFF-0016128
120.	POL00394008	Problem Management, Status Report, August 2001	POL-BSFF-0220678
121.	POL00178062	Problem Management, Status Report, October 2001	POL-BSFF-0016125
122.	POL00393981	ICL Pathway Problem Management Procedures, Version 1.0, 30 January 2001	POL-BSFF-0220651
123.	POL00393981	ICL Pathway Problem Management Procedures, Version 1.0, 30 January 2001	POL-BSFF-0220651
124.	POL00397084	RMGA Customer Service Incident Management Process, 28 July 2009	POL-BSFF-0223754
125.	POL00397084	RMGA Customer Service Incident Management Process, 28 July 2009	POL-BSFF-0223754
126.	POL00396892	Security Testing Inputs for PCI Audit, 01 August 2008	POL-BSFF-0223562
127.	POL00398421	HNG-X Architecture - Security Architecture, 24 September 2014	POL-BSFF-0225091
128.	POL00398421	HNG-X Architecture - Security Architecture, 24 September 2014	POL-BSFF-0225091
129.	POL00398421	HNG-X Architecture - Security Architecture, 24 September 2014	POL-BSFF-0225091
130.	POL00399608	PCI DSS - Quarterly ASV Scan detailed report, 2 October 2015	POL-BSFF-0226278
131.	POL00396892	Security Testing Inputs for PCI Audit, 1 August 2008	POL-BSFF-0223562
132.	POL00397485	Penetration Testing Policy, 24 October 2011	POL-BSFF-0224155
133.	POL00401615	Audit, Risk and Compliance Committee Papers, 24 November 2020	POL-BSFF-0228285
134.	POL00399707	Branch Counter Refresh Test Strategy, 29 February 2016	POL-BSFF-0226377
135.	POL00396892	Security Testing Inputs for PCI Audit, 1 August 2008	POL-BSFF-0223562

WITN03680200

136.	POL00398165	Network Security High Level Design, 6 September 2007	POL-BSFF-0224835
137.	POL00398922	HNG-X System Qualities Architecture, 25 March 2011	POL-BSFF-0225592
138.	POL00398924	HNG-X Architecture - Security Architecture, 24 September 2014	POL-BSFF-0225594
139.	POL00399062	HNG-X Counter Architecture, 19 August 2011	POL-BSFF-0225732
140.	POL00399072	HNG-X System Qualities Architecture, 25 March 2011	POL-BSFF-0225742
141.	POL00393859	Post Office Payment Service, Customer Solution Proposal, 15 February 2017	POL-BSFF-0220537
142.	POL00393766	Schedule 22, PCI Compliance, (undated)	POL-BSFF-0220444
143.	POL00399212	HNG-X Counter Architecture, 19 August 2011	POL-BSFF-0225882
144.	POL00397094	HNG-X Resilience and Disaster Recovery High Level Design, 23 July 2008	POL-BSFF-0223764
145.	POL00397348	IT & Change Weekly Project Highlight Report - PCI DSS Compliance, 11 January 2012	POL-BSFF-0224018
146.	POL00397418	Post Office Invitation to Tender, 28 May 2012	POL-BSFF-0224088
147.	POL00397450	Post Office IT Solutions Framework, 15 June 2012	POL-BSFF-0224120
148.	POL00401512	IT Delivery Portfolio, Project Initiation Document, 10 October 2014	POL-BSFF-0228182
149.	POL00397159	Low Level Design For the DCS Authorisation Agent, 20 August 2009	POL-BSFF-0223829
150.	POL00397162	Sysman Support Tasks for HNG-X, 7 September 2009	POL-BSFF-0223832
151.	POL00397163	TPS HNG-X Application Changes Low Level Design, 22 June 2007	POL-BSFF-0223833
152.	POL00397165	TPS HNG-X Application Changes Low Level Design, 22 June 2007	POL-BSFF-0223835
153.	POL00397360	HNG X Programme, PCI Incident Response Plan, 6 December 2010	POL-BSFF-0224030
154.	POL00324854	Change Control Note No 1202, 7 August 2003	POL-BSFF-0162600
155.	POL00396909	Weekly Highlight Report - PCI Compliance - HNG-X & BP Sales, 8 August 2008-15 October 2008	POL-BSFF-0223579
156.	POL00396887	Weekly Highlight Report - PCI Compliance - HNG-X & BP Sales, 25 July 2008-1 August 2008	POL-BSFF-0223557
157.	POL00397377	HNG X Programme, PCI Incident Response Plan, November 2011	POL-BSFF-0224047
158.	POL00256092	Terms of Reference for Post Office Account (POA) Business Impact Forum (BIF) and Peak Targeting Forum (PTF), Version 1, 30 July 2014	POL-BSFF-0094155
159.	POL00400641	Terms of Reference for Post Office Account (POA) Business Impact Forum (BIF) and Peak Targeting Forum (PTF), Version 1, 30 July 2014	POL-BSFF-0227311
160.	POL00401529	Post Office Limited Technical CAB Minutes, 3 September 2019	POL-BSFF-0228199
161.	POL00398051	Post Office IT&C Transformation Project Procurement Guide, 13 November 2013	POL-BSFF-0224721

WITN03680200

162.	POL00401616	Investment Committee Papers, 7 December 2020	POL-BSFF-0228286
163.	POL00398109	SISD Governance Model, Terms of Reference, Version 1, 31 March 2014	POL-BSFF-0224779
164.	POL00398100	SISD Governance Model, Terms of Reference, Version 0.16, 21 March 2014	POL-BSFF-0224770
165.	POL00398100	SISD Governance Model, Terms of Reference, Version 0.16, 21 March 2014	POL-BSFF-0224770
166.	POL00398100	SISD Governance Model, Terms of Reference, Version 0.16, 21 March 2014	POL-BSFF-0224770
167.	POL00398100	SISD Governance Model, Terms of Reference, Version 0.16, 21 March 2014	POL-BSFF-0224770
168.	POL00399459	ATOS, Post Office Limited Security Management Plan, Version 1.0, March 2015	POL-BSFF-0226129
169.	POL00401508	ATOS, Post Office Limited Security Management Plan, Version 1.0 (draft), July 2013	POL-BSFF-0228178
170.	POL00401508	ATOS, Post Office Limited Security Management Plan, Version 1.0 (draft), July 2013	POL-BSFF-0228178
171.	POL00401508	ATOS, Post Office Limited Security Management Plan, Version 1.0 (draft), July 2013	POL-BSFF-0228178
172.	POL00397409	IT & Change Weekly Highlight Report, 29 April 2012	POL-BSFF-0224079
173.	POL00397440	IT & Change Weekly Highlight Report, 27 May 2012	POL-BSFF-0224110
174.	POL00397379	IT & Change Weekly Highlight Report, 24 February 2012	POL-BSFF-0224049
175.	POL00399501	SISD Risk Log (Interim), SISD Risk Management Process, 1 April 2014	POL-BSFF-0226171
176.	POL00397903	IT&C Transformation Programme, Executive Dashboard, 14 December 2012	POL-BSFF-0224573
177.	POL00397925	IT&C Transformation Programme, Executive Dashboard, 18 January 2013	POL-BSFF-0224595
178.	POL00325396	Post Office Limited Service Level Tracker, 26 May 2017	POL-BSFF-0163142
179.	POL00398086	Post Office SISD Contract Handbook, Version 2, 28 January 2014	POL-BSFF-0224756
180.	POL00399522	SISD Risk Log (Interim), SISD Risk Management Process, 1 April 2014	POL-BSFF-0226192
181.	POL00400226	ATOS Consolidated Service Review Report, 23 March 2017	POL-BSFF-0226896
182.	POL00399592	ATOS Consolidated Service Review Report, August 2015	POL-BSFF-0226262
183.	POL00399751	M4 Governance Meeting, 3 May 2016	POL-BSFF-0226421
184.	POL00399522	SISD Risk Log (Interim), SISD Risk Management Process, 1 April 2014	POL-BSFF-0226192
185.	POL00399525	Post Office Limited Service Level Tracker, 20 February 2015	POL-BSFF-0226195

WITN03680200

186.	POL00397932	Operational Business Change - Branch Operational Level Agreement, 1 November 2011	POL-BSFF-0224602
187.	POL00397971	Fujitsu Services (Pathway) Ltd/Post Office Ltd Interface Agreement for Operational Business Change - Product, 9 August 2013	POL-BSFF-0224641
188.	POL00397971	Fujitsu Services (Pathway) Ltd/Post Office Ltd Interface Agreement for Operational Business Change - Product, 9 August 2013	POL-BSFF-0224641
189.	POL00397971	Fujitsu Services (Pathway) Ltd/Post Office Ltd Interface Agreement for Operational Business Change - Product, 9 August 2013	POL-BSFF-0224641
190.	POL00397971	Fujitsu Services (Pathway) Ltd/Post Office Ltd Interface Agreement for Operational Business Change - Product, 9 August 2013	POL-BSFF-0224641
191.	POL00397971	Fujitsu Services (Pathway) Ltd/Post Office Ltd Interface Agreement for Operational Business Change - Product, 9 August 2013	POL-BSFF-0224641
192.	POL00397971	Fujitsu Services (Pathway) Ltd/Post Office Ltd Interface Agreement for Operational Business Change - Product, 9 August 2013	POL-BSFF-0224641
193.	POL00393768	Security Management Service: Service Description, 4 April 2014	POL-BSFF-0220446
194.	POL00395097	Fujitsu Services Royal Mail Group Account Information Security Management System Policy Set - Security Incident Management, Version 0.1, 3 September 2007	POL-BSFF-0221767
195.	POL00393768	Security Management Service: Service Description, 4 April 2014	POL-BSFF-0220446
196.	POL00398421	HNG-X Architecture - Security Architecture, 24 September 2014	POL-BSFF-0225091
197.	POL00235089	Description of Fujitsu's System of IT Infrastructure Services supporting Post Office Limited's POLSAP and HNG-X applications. Document includes the independent service auditor's assurance report including tests performed and results thereof, 12 February 2014	POL-BSFF-0073152
198.	POL00399609	"Description of Fujitsu's System of IT Infrastructure Services supporting Post Office Limited's POLSAP and HNG-X applications". This document includes the independent service auditor's assurance report including tests performed and results thereof, 7 October 2015	POL-BSFF-0226279
199.	POL00401517	Fujitsu Services/Post Office Limited Interface Agreement for the Problem Management Interface, 09 March 2016	POL-BSFF-0228187
200.	POL00401517	Fujitsu Services/Post Office Limited Interface Agreement for the Problem Management Interface, 09 March 2016	POL-BSFF-0228187
201.	POL00393885	Service Management Framework - Incident Management, 18 August 1999	POL-BSFF-0220555
202.	POL00401517	Fujitsu Services/Post Office Limited Interface Agreement for the Problem Management Interface, 09 March 2016	POL-BSFF-0228187
203.	POL00137533	Weekly Horizon Call - Terms of Reference, 24 September 2013	POL-BSFF-0000191

WITN03680200

204.	POL00397399	Audit, Risk and Compliance Sub-Committee Terms of Reference, 12 April 2012	POL-BSFF-0224069
205.	POL00401627	Risk and Compliance Committee Agenda and Papers, 10 July 2018	POL-BSFF-0228297
206.	POL00401626	Risk and Compliance Committee Agenda and Papers, 13 March 2018	POL-BSFF-0228296
207.	POL00401628	Risk and Compliance Committee Agenda and Papers, 14 January 2020	POL-BSFF-0228298
208.	POL00401629	Risk and Compliance Committee Agenda and Papers, 10 September 2020	POL-BSFF-0228299
209.	POL00400766	Investment Committee Papers, 14 November 2018	POL-BSFF-0227436
210.	POL00400766	Risk and Compliance Committee Agenda and Papers, 13 March 2018	POL-BSFF-0227436
211.	POL00401625	Risk and Compliance Committee Agenda and Papers, 20 July 2017	POL-BSFF-0228295
212.	POL00400133	CIO Risk Log, October 2016	POL-BSFF-0226803
213.	POL00400101	Audit, Risk and Compliance Committee Agenda and Minutes, 28 September 2016	POL-BSFF-0226771
214.	POL00400101	Audit, Risk and Compliance Committee Agenda and Minutes, 28 September 2016	POL-BSFF-0226771
215.	POL00401624	Risk and Compliance Committee Agenda and Papers, 4 May 2017	POL-BSFF-0228294
216.	POL00401616	Investment Committee Papers, 7 December 2020	POL-BSFF-0228286
217.	POL00400632	Post Office Limited Internal Audit Report - Branch Technology, 4 July 2018	POL-BSFF-0227302
218.	POL00400397	Post Office Limited Internal Audit Report - Branch Technology, 2 July 2018	POL-BSFF-0227067
219.	POL00400632	Post Office Limited Internal Audit Report - Branch Technology, 4 July 2018	POL-BSFF-0227302
220.	POL00397400	IT&C Transformation Programme Board Update, 16 April 2012	POL-BSFF-0224070
221.	POL00400226	ATOS Consolidated Service Review Report, 23 March 2017	POL-BSFF-0226896
222.	POL00399592	ATOS Consolidated Service Review Report, August 2015	POL-BSFF-0226262
223.	POL00399751	M4 Governance Meeting, 3 May 2016	POL-BSFF-0226421
224.	POL00399522	SISD Risk Log (Interim), SISD Risk Management Process, 1 April 2014	POL-BSFF-0226192
225.	POL00399525	Post Office Limited Service Level Tracker, 20 February 2015	POL-BSFF-0226195
226.	POL00393769	Schedule B6.3, HNG-X Acceptance Process, (undated)	POL-BSFF-0220447
227.	POL00393769	Schedule B6.3, HNG-X Acceptance Process, (undated)	POL-BSFF-0220447
228.	POL00393769	Schedule B6.3, HNG-X Acceptance Process, (undated)	POL-BSFF-0220447
229.	POL00325152	Schedule B6.3, HNG-X Acceptance Process, 22 December 2021	POL-BSFF-0162898
230.	POL00398082	Post Office/Fujitsu Executive Steering Board Agenda, 23 January 2014	POL-BSFF-0224752
231.	POL00400086	Post Office/Fujitsu Executive Steering Board Agenda, August 2016	POL-BSFF-0226756
232.	POL00398082	Post Office/Fujitsu Executive Steering Board Agenda, 23 January 2014	POL-BSFF-0224752

WITN03680200

233.	POL00398561	Post Office/Fujitsu Executive Steering Board Agenda, 7 January 2015	POL-BSFF-0225231
234.	POL00400086	Post Office/Fujitsu Executive Steering Board Agenda, August 2016	POL-BSFF-0226756
235.	POL00400086	Post Office/Fujitsu Executive Steering Board Agenda, August 2016	POL-BSFF-0226756
236.	POL00398561	Post Office/Fujitsu Executive Steering Board Agenda, 7 January 2015	POL-BSFF-0225231
237.	POL00400086	Post Office/Fujitsu Executive Steering Board Agenda, August 2016	POL-BSFF-0226756
238.	POL00400076	Post Office/Fujitsu, Executive Steering Board Agenda, July 2016	POL-BSFF-0226746
239.	POL00353031	Post Office Limited Board Meeting Papers, 25 March 2015	POL-BSFF-0178752
240.	POL00353031	Post Office Limited Board Meeting Papers, 25 March 2015	POL-BSFF-0178752
241.	POL00399587	Post Office Limited Board Meeting Minutes, 25 July 2016	POL-BSFF-0226257
242.	POL00242846	Branch Network, Business IT Performance, 22 June 2016	POL-BSFF-0080909
243.	POL00400007	Email from Andy Garner (Post Office Limited) to Rob Houghton (Post Office Limited) and Sharon Gilkes (Post Office Limited) re Network Business IT Performance Slides, 21 June 2016	POL-BSFF-0226677
244.	POL00242845	Email from Andy Garner (Post Office Limited) to Angela Van-Den-Bogerd (Post Office Limited) and others re Service Slides, 22 June 2016	POL-BSFF-0080908
245.	POL00400037	Email from Andy Garner (Post Office Limited) to Rob Houghton (Post Office Limited), Sharon Gilkes (Post Office Limited) and others re Network Business IT Performance Slides, 20 July 2016	POL-BSFF-0226707
246.	POL00401507	CIO Operations Board Meeting, 25 July 2016	POL-BSFF-0228177
247.	POL00400116	Email from Andy Garner (Post Office Limited) to Angela Van-Den-Bogerd (Post Office Limited) and others re IT Operating Performance slides, 19 October 2016	POL-BSFF-0226786
248.	POL00401507	CIO Operations Board Meeting, 25 July 2016	POL-BSFF-0228177
249.	POL00400133	CIO Risk Log, October 2016	POL-BSFF-0226803
250.	POL00398199	Information Security Committee Agenda, Minutes and Action Points, 5 June 2014	POL-BSFF-0224869
251.	POL00393731	Information Security Review, POca End-to-End Information Security, Technology and Product Process Risk Review, 13 February 2013	POL-BSFF-0220409
252.	POL00400810	Access Control Policy, Version 1, 17 April 1997	POL-BSFF-0227480
253.	POL00400776	Access Control Policy, Version 4, 16 July 2002	POL-BSFF-0227446
254.	POL00394858	Reconciliation Service: Service Description, 24 August 2006	POL-BSFF-0221528
255.	POL00393950	ICL Pathway TPS Reconciliation & Incident Management, Version 1.0, 16 October 2000	POL-BSFF-0220620

WITN03680200

256.	POL00394858	Reconciliation Service: Service Description, 24 August 2006	POL-BSFF-0221528
257.	POL00394858	Reconciliation Service: Service Description, 24 August 2006	POL-BSFF-0221528
258.	POL00400387	Reconciliation Service: Service Description, 3 December 2013	POL-BSFF-0227057
259.	POL00394858	Reconciliation Service: Service Description, 24 August 2006	POL-BSFF-0221528
260.	POL00400387	Reconciliation Service: Service Description, 3 December 2013	POL-BSFF-0227057
261.	POL00401578	Reconciliation Service: Service Description, 3 June 2020	POL-BSFF-0228248
262.	POL00397112	HNG-X Technical Security Architecture, Version 2, 8 January 2009	POL-BSFF-0223782
263.	POL00400323	HNG-X/HNG-A Architecture - Security Architecture, 12 July 2017	POL-BSFF-0226993
264.	POL00400840	CS Support Services Operations Manual, 7 November 2000	POL-BSFF-0227510
265.	POL00401505	Operations Manual for the Customer Service Directorate, Version 0.2, 22 November 2001	POL-BSFF-0228175
266.	POL00400793	Access Control Policy, Version 3, 18 December 1998	POL-BSFF-0227463
267.	POL00400795	Access Control Policy, Version 3.1, 18 February 2002	POL-BSFF-0227465
268.	POL00400792	Access Control Policy, Version 3.4, 18 February 2002	POL-BSFF-0227462
269.	POL00400791	Access Control Policy, Version 6.0, 8 August 2003	POL-BSFF-0227461
270.	POL00400790	Access Control Policy, Version 7, 14 April 2005	POL-BSFF-0227460
271.	POL00400799	Access Control Policy, Version 2, 24 February 1998	POL-BSFF-0227469
272.	POL00400799	Access Control Policy, Version 2, 24 February 1998	POL-BSFF-0227469
273.	POL00400799	Access Control Policy, Version 2, 24 February 1998	POL-BSFF-0227469
274.	POL00400799	Access Control Policy, Version 2, 24 February 1998	POL-BSFF-0227469
275.	POL00400810	Access Control Policy, Version 1, 17 April 1997	POL-BSFF-0227480
276.	POL00400810	Access Control Policy, Version 1, 17 April 1997	POL-BSFF-0227480
277.	POL00394877	HNG-X Technical Security Architecture, Version 1, 16 February 2007	POL-BSFF-0221547
278.	POL00394583	Post Office Community Information Security Policy for Horizon, Version 1.0, 8 June 2005	POL-BSFF-0221253
279.	POL00397117	Community Information Security Policy for Horizon & Horizon Online, Version 2.0, 22 March 2010	POL-BSFF-0223787
280.	POL00397136	Community Information Security Policy for Horizon & Horizon Online, Version 3.0, 24 August 2010	POL-BSFF-0223806
281.	POL00397343	Community Information Security Policy for Horizon & Horizon Online, Version 4.0, 13 October 2011	POL-BSFF-0224013
282.	POL00401642	Horizon Security Policy, 24 February 2006	POL-BSFF-0228312

WITN03680200

283.	POL00401642	Horizon Security Policy, 24 February 2006	POL-BSFF-0228312
284.	POL00400809	Access Control Policy, Version 7.1, 2 June 2009	POL-BSFF-0227479
285.	POL00397052	Security Management Service: Service Description, Version 2.0, 31 December 2008	POL-BSFF-0223722
286.	POL00401642	Horizon Security Policy, 24 February 2006	POL-BSFF-0228312
287.	POL00401642	Horizon Security Policy, 24 February 2006	POL-BSFF-0228312
288.	POL00401199	Access Control Policy, Version 3, 18 December 1998	POL-BSFF-0227869
289.	POL00401199	Access Control Policy, Version 3, 18 December 1998	POL-BSFF-0227869
290.	POL00400776	Access Control Policy, Version 4, 16 July 2002	POL-BSFF-0227446
291.	POL00400776	Access Control Policy, Version 4, 16 July 2002	POL-BSFF-0227446
292.	POL00400776	Access Control Policy, Version 4, 16 July 2002	POL-BSFF-0227446
293.	POL00400776	Access Control Policy, Version 4, 16 July 2002	POL-BSFF-0227446
294.	POL00397112	HNG-X Technical Security Architecture, Version 2, 8 January 2009	POL-BSFF-0223782
295.	POL00400667	Remote Support Secure Access Server High Level Design, Version 3, 24 October 2016	POL-BSFF-0227337
296.	POL00225860	Fujitsu Post Office Account User Access Procedure, Version 4.0, 18 October 2011	POL-BSFF-0063923
297.	POL00394877	HNG-X Technical Security Architecture, Version 1, 16 February 2007	POL-BSFF-0221547
298.	POL00398825	HNG-X Counter Architecture, Version 4.0, 19 August 2011	POL-BSFF-0225495
299.	POL00400667	Remote Support Secure Access Server High Level Design, Version 3, 24 October 2016	POL-BSFF-0227337
300.	POL00400840	CS Support Services Operations Manual, 7 November 2000	POL-BSFF-0227510
301.	POL00400840	CS Support Services Operations Manual, 7 November 2000	POL-BSFF-0227510
302.	POL00401116	End to End Application Support Strategy, Version 1.0, 28 July 2011	POL-BSFF-0227786
303.	POL00400776	Access Control Policy, Version 4, 16 July 2002	POL-BSFF-0227446
304.	POL00400810	Access Control Policy, Version 1, 17 April 1997	POL-BSFF-0227480
305.	POL00400776	Access Control Policy, Version 4, 16 July 2002	POL-BSFF-0227446
306.	POL00401619	ICL Pathway Audit Trail Functional Specification, Version 3.0, 1 July 1999	POL-BSFF-0228289
307.	POL00393978	ICL Pathway Audit Trail Functional Specification Version 5.0, 15 January 2001	POL-BSFF-0220648
308.	POL00400840	CS Support Services Operations Manual, 7 November 2000	POL-BSFF-0227510
309.	POL00400835	Operations Manual for the Customer Service Directorate, Version 1, 26 November 2001	POL-BSFF-0227505

WITN03680200

310.	POL00401505	Operations Manual for the Customer Service Directorate, Version 0.2, 22 November 2001	POL-BSFF-0228175
311.	POL00400835	Operations Manual for the Customer Service Directorate, Version 1, 26 November 2001	POL-BSFF-0227505
312.	POL00400776	Access Control Policy, Version 4, 16 July 2002	POL-BSFF-0227446
313.	POL00400835	Operations Manual for the Customer Service Directorate, Version 1, 26 November 2001	POL-BSFF-0227505
314.	POL00400790	Access Control Policy, Version 7, 14 April 2005	POL-BSFF-0227460
315.	POL00401642	Horizon Security Policy, 24 February 2006	POL-BSFF-0228312
316.	POL00401642	Horizon Security Policy, 24 February 2006	POL-BSFF-0228312
317.	POL00394877	HNG-X Technical Security Architecture, Version 1, 16 February 2007	POL-BSFF-0221547
318.	POL00397112	HNG-X Technical Security Architecture, Version 2, 8 January 2009	POL-BSFF-0223782
319.	POL00400323	HNG-X/HNG-A Architecture – Security Architecture, 12 July 2017	POL-BSFF-0226993
320.	POL00401116	End to End Application Support Strategy, Version 1.0, 28 July 2011	POL-BSFF-0227786
321.	POL00401116	End to End Application Support Strategy, Version 1.0, 28 July 2011	POL-BSFF-0227786
322.	POL00396665	Remote Support Secure Access Server High Level Design, Version 2, 13 May 2008	POL-BSFF-0223335
323.	POL00395680	Remote Support Secure Access Server High Level Design, Version 1, 10 January 2008	POL-BSFF-0222350
324.	POL00397112	HNG-X Technical Security Architecture, Version 2, 8 January 2009	POL-BSFF-0223782
325.	POL00394877	HNG-X Technical Security Architecture, Version 1, 16 February 2007	POL-BSFF-0221547
326.	POL00396665	Remote Support Secure Access Server High Level Design, Version 2, 13 May 2008	POL-BSFF-0223335
327.	POL00396665	Remote Support Secure Access Server High Level Design, Version 2, 13 May 2008	POL-BSFF-0223335
328.	POL00397089	Branch Database High Level Design, Version 1, 17 November 2009	POL-BSFF-0223759
329.	POL00397089	Branch Database High Level Design, Version 1, 17 November 2009	POL-BSFF-0223759
330.	POL00397089	Branch Database High Level Design, Version 1, 17 November 2009	POL-BSFF-0223759
331.	POL00401510	Security Management Service: Service Description, Version 5.0, 4 April 2014	POL-BSFF-0228180
332.	POL00401509	Security Management Service: Service Description, Version 5.1, 3 March 2015	POL-BSFF-0228179
333.	POL00031407	Description of Fujitsu's System of IT Infrastructure Services supporting Post Office Limited's POLSAP and HNG-X applications. Document includes the independent service auditor's assurance report including tests performed and results thereof, 15 February 2013	POL-0028309
334.	POL00031407	Description of Fujitsu's System of IT Infrastructure Services supporting Post Office Limited's POLSAP and HNG-X	POL-0028309

WITN03680200

		applications. Document includes the independent service auditor's assurance report including tests performed and results thereof, 15 February 2013	
335.	POL00398087	Description of Fujitsu's System of IT Infrastructure Services supporting Post Office Limited's POLSAP and HNG-X applications. Document includes the independent service auditor's assurance report including tests performed and results thereof, 13 February 2014	POL-BSFF-0224757
336.	POL00401632	Email from Kay Alastair (Fujitsu) to Kathryn Alexander (Post Office Limited) re Access to Information in Branch for transaction logs, 21 February 2014	POL-BSFF-0228302
337.	POL00394026	ICL Pathway Audit of the Horizon Data Centres and Belfast Operations Centre, Version 2, 21 November 2001	POL-BSFF-0220696
338.	POL00396456	Ernst & Young Audit Results Report, 7 May 2008	POL-BSFF-0223126
339.	POL00396009	Post Office Audit and Risk Committee Minutes and Papers, 6 March 2008	POL-BSFF-0222679
340.	POL00396455	Post Office Audit and Risk Committee Minutes and Papers, 7 May 2008	POL-BSFF-0223125
341.	POL00396890	Presentation for Post Office Audit Committee, IT Governance Review, 3 September 2008	POL-BSFF-0223560
342.	POL00030261	Ernst & Young Audit Results Report, 13 May 2010	POL-0026743
343.	POL00030261	Ernst & Young Audit Results Report, 13 May 2010	POL-0026743
344.	POL00030261	Ernst & Young Audit Results Report, 13 May 2010	POL-0026743
345.	POL00030217	Ernst & Young Management Letter for Year Ended 27 March 2011, August 2011	POL-0026699
346.	POL00030217	Ernst & Young Management Letter for Year Ended 27 March 2011, August 2011	POL-0026699
347.	POL00030217	Ernst & Young Management Letter for Year Ended 27 March 2011, August 2011	POL-0026699
348.	POL00030217	Ernst & Young Management Letter for Year Ended 27 March 2011, August 2011	POL-0026699
349.	POL00030217	Ernst & Young Management Letter for Year Ended 27 March 2011, August 2011	POL-0026699
350.	POL00030217	Ernst & Young Management Letter for Year Ended 27 March 2011, August 2011	POL-0026699
351.	POL00030217	Ernst & Young Management Letter for Year Ended 27 March 2011, August 2011	POL-0026699
352.	POL00238126	Ernst and Young Control Themes and Observations Arising from the 2010-11 Audit, 15 November 2011	POL-BSFF-0076189
353.	POL00029438	Post Office Board, Post Office Limited IT Audit Update (SAS70), September 2011	POL-0025920
354.	POL00142943	Email thread between Sarah Hall (Post Office Limited), Lesley Sewell (Post Office Limited) and Neil Lecky-Thompson (Post Office Limited) re EY audit - management letter points, 21 March 2012	POL-BSFF-0002108

WITN03680200

355.	POL00142944	Management Response and Summary of Ernst & Young Financial Audit Findings 2011/12, (undated)	POL-BSFF-0002109
356.	POL00142948	Review of Key System Controls in Horizon, Post Office Limited, March 2012	POL-BSFF-0002113
357.	POL00143038	Ernst & Young Audit Results Report, 10 May 2012	POL-BSFF-0002203
358.	POL00397495	Post Office Risk and Compliance Committee presentation regarding the Ernst & Young 2011-12 Management Letter, 14 May 2012	POL-BSFF-0224165
359.	POL00143524	Email from Sarah Hall (Post Office Limited) to Rod Ismay (Post Office Limited) and Lesley Sewell (Post Office Limited) forwarding email from Jeremy Midkiff (Ernst & Young) re Post Office Limited Management Letter, 9 August 2012	POL-BSFF-0002689
360.	POL00143525	Ernst & Young Control Themes and Observations from 2012 Audit, 13 August 2012	POL-BSFF-0002690
361.	POL00143525	Ernst & Young Control Themes and Observations from 2012 Audit, 13 August 2012	POL-BSFF-0002690
362.	POL00397878	Post Office Risk and Compliance Committee Meeting Minutes, 17 September 2012.	POL-BSFF-0224548
363.	POL00397899	Risk and Compliance Committee Paper regarding the 2011/12 IT Annual Audit Update, 23 November 2012	POL-BSFF-0224569
364.	POL00397899	Risk and Compliance Committee Paper regarding the 2011/12 IT Annual Audit Update, 23 November 2012	POL-BSFF-0224569
365.	POL00398154	Post Office Follow Up Review of Key System Controls in Horizon – Assurance Review, December 2012	POL-BSFF-0224824
366.	POL00397990	Post Office Audit, Risk and Compliance Sub-Committee Meeting Minutes, 12 September 2013	POL-BSFF-0224660
367.	POL00137294	Email thread between Paula Vennells (Post Office Limited), Chris Day (Post Office Limited), Lesley Sewell (Post Office Limited), Susan Crichton (Post Office Limited), Susan Barton (Post Office Limited), and Sarah Hall (Post Office Limited) re Management Control Audit - SAS70 for Fujitsu, 2 March 2013	POL-BSFF-0000065
368.	POL00026621	Description of Fujitsu's System of IT Infrastructure Services Supporting Post Office Limited's POLSAP and HNG-X Applications, 1 April 2012 to 31 December 2012	POL-0023262

WITN03680200

369.	POL00144637	Post Office Audit, Risk and Compliance Sub-Committee Meeting Minutes and Papers, 21 May 2013	POL-BSFF-0003768
370.	POL00398154	Post Office Follow Up Review of Key System Controls in Horizon – Assurance Review, December 2012	POL-BSFF-0224824
371.	POL00021524	Post Office Limited Board Minutes, 30 April 2014	POL0000057
372.	POL00399614	Deloitte Board Briefing - Document, further to our report 'Horizon: Desktop review of assurance sources and key control features' dated 23/5/14, responding to five specific matters identified by Post Office Limited as critical to Post Office Limited's legal position, 4 June 2014	POL-BSFF-0226284
373.	POL00030451	Deloitte Board Briefing - Document, further to our report 'Horizon: Desktop review of assurance sources and key control features' dated 23/5/14, responding to five specific matters identified by Post Office Limited as critical to Post Office Limited's legal position, 4 June 2014	POL-0026933
374.	POL00401635	Post Office Limited, Action Summary, 12 June 2014	POL-BSFF-0228305
375.	POL00206524	Risk and Compliance Committee Meeting Agenda, Minutes and Papers, 21 July 2014	POL-BSFF-0044587
376.	POL00401633	CIO Risk Log, April 2016	POL-BSFF-0228303
377.	POL00030452	A Review on Behalf of the Chairman of Post Office Limited - Concerning the Steps Taken in Response to Various Complaints Made by Sub-Postmasters, 8 February 2016	POL-0026934
378.	POL00029984	Deloitte LLP, Sparrow - Interim Report (Draft for discussion), 8 July 2016	POL-0026466
379.	POL00400064	'Bramble' - Interim Report, 27 July 2016	POL-BSFF-0226734
380.	POL00400125	'Bramble' - Draft Report, 31 October 2016	POL-BSFF-0226795
381.	POL00401550	'Bramble' - Draft Report, 3 October 2017	POL-BSFF-0228220
382.	POL00400287	'Bramble' - Draft Report, 15 December 2017	POL-BSFF-0226957
383.	POL00401634	Description of Fujitsu's System of IT Infrastructure Services Supporting Post Office Limited's POLSAP and HNG-X Applications, 1 April 2017 to 31 December 2017	POL-BSFF-0228304
384.	POL00253246	'Bramble' - Draft Report, 19 January 2018	POL-BSFF-0091309
385.	POL00401577	Audit, Risk and Compliance Committee Agenda and Papers, 19 May 2020	POL-BSFF-0228247
386.	POL00401577	Audit, Risk and Compliance Committee Agenda and Papers, 19 May 2020	POL-BSFF-0228247
387.	POL00031727	KPMG Horizon Audit - Interim report into the progress made to address six HITJ Report issues (Draft), 16 December 2020	POL-0028629

WITN03680200

388.	POL00401675	IT Contract Manager Job Description, April 2018	POL-BSFF-0228345
389.	POL00401676	Solutions Architect Job Description, (undated)	POL-BSFF-0228346
390.	POL00401677	Solutions Architect Job Description, (undated)	POL-BSFF-0228347
391.	POL00401678	Domain CTO - FS&T Job Description, (undated)	POL-BSFF-0228348
392.	POL00401679	Senior Business Analyst Job Description, (undated)	POL-BSFF-0228349
393.	POL00401680	Service Delivery Manager, Data Services Job Description, (undated)	POL-BSFF-0228350
394.	POL00400777	Service Level Targets for Horizon Services, 5 December 2002	POL-BSFF-0227447
395.	FUJ00080297	Calculation of SLT of Branch and Counter Unavailability, (undated)	POINQ0086468F
396.	FUJ00234704	Invoice Request Q3, Horizon Service Credits, October 2007 to December 2007	POINQ0240847F
397.	POL00337672	Post Office Limited Board Report, 17 January 2024	POL-BSFF-0190574
398.	POL00337701	Horizon Issues Remediation Programme - HIJ Progress Summary, December 2023	POL-BSFF-0190603
399.	POL00337565	Post Office Limited Test Strategy, 24 May 2022	POL-BSFF-0190467
400.	POL00337564	Horizon report - Report on the progress made to address six areas derived from HIJ findings, June 2021	POL-BSFF-0190466
401.	POL00030528	The BED Report, (undated)	POL-0027010
402.	POL00337673	Historic KELS Determination and Closure, 28 June 2021	POL-BSFF-0190575
403.	POL00337594	Branch Impacting Problems - Latest Status of Open Items, (undated)	POL-BSFF-0190496
404.	POL00337571	Defect Report - Latest status of Open Items, July 2023	POL-BSFF-0190473
405.	POL00337574	Branch Impacting Problems - Latest Status of Open Items, August 2023	POL-BSFF-0190476
406.	POL00337575	Branch Impacting Problems - Latest Status of Open Items, September 2023	POL-BSFF-0190477
407.	POL00337590	Horizon Problems - Latest Status of Open Items, 2 October 2023	POL-BSFF-0190492
408.	POL00337570	Defect Report - Latest Status of Open Items, 12 June 2023	POL-BSFF-0190472
409.	POL00337616	Horizon Problems - Latest Status of Open Items, December 2023	POL-BSFF-0190518
410.	POL00337618	Horizon Problems - Latest Status of Open Items, January 2024	POL-BSFF-0190520
411.	POL00337563	Verizon Alerts: Recommendation Summary, (undated)	POL-BSFF-0190465
412.	POL00337591	Post Office IT Major Incident Management Standard Operating Procedure, Version 1.1, 24 July 2023	POL-BSFF-0190493
413.	POL00337622	Contract Management Framework - For Post Office and its Group Companies, 24 August 2021	POL-BSFF-0190524
414.	FUJ00000071	Codified Agreement between Post Office Counters Limited and ICL Pathway Limited, 28 July 1999	POINQ0006242F

WITN03680200

415.	POL00325247	Schedule A2, Version 14 – Relationship and Governance (undated)	POL-BSFF-0162993
416.	POL00337671	Documentation Map – All Horizon IT depts	POL-BSFF-0190573
417.	POL00337642	CIO Policies Application Architecture Policy Version 1.1, (undated)	POL-BSFF-0190544
418.	POL00337649	Horizon Solution Architecture Outline, 7 April 2016	POL-BSFF-0190551
419.	POL00337643	Architecture & Design Principles, (undated)	POL-BSFF-0190545
420.	POL00337562	Architecture Governance Post Office IT (undated)	POL-BSFF-0190464
421.	POL00337615	Horizon Solution Architecture Outline, 27 September 2023	POL-BSFF-0190517
422.	POL00337647	Horizon Improvements Programme, January 2021	POL-BSFF-0190549
423.	POL00337648	Horizon System Improvements Process Guide, (undated)	POL-BSFF-0190550
424.	POL00337646	Post Office Architecture Governance, (undated)	POL-BSFF-0190548
425.	POL00337645	CTO Principles, Guidelines and Patterns, 28 May 2019	POL-BSFF-0190547
426.	POL00337644	CTO Principles, Guidelines and Patterns, 9 October 2018	POL-BSFF-0190546
427.	POL00337627	Contract Approval Process, (undated)	POL-BSFF-0190529
428.	POL00337669	IT Contract Breach Management Process, (undated)	POL-BSFF-0190571
429.	POL00337664	Contract Conformance, (undated)	POL-BSFF-0190566
430.	POL00337663	Post Office Limited - Procurement to IT Contract Manager Handover, (undated)	POL-BSFF-0190565
431.	POL00337665	Contract Interpretation, 20 March 2018	POL-BSFF-0190567
432.	POL00337626	Contract Management Team Contract Approval IT Quick Reference Guide, March 2021	POL-BSFF-0190528
433.	POL00337622	Contract Management Framework - For Post Office and its Group Companies, 24 August 2021	POL-BSFF-0190524
434.	POL00337670	Contract & Vendor Management - RACI Model, August 2020	POL-BSFF-0190572
435.	POL00337667	Supplier Exit and Transition Planning, 10 July 2018	POL-BSFF-0190569
436.	POL00337666	CVM Planning - Exit Management (Strategy & Planning), (undated)	POL-BSFF-0190568
437.	POL00337624	IT Supplier Tiering User Guidance, (undated)	POL-BSFF-0190526
438.	POL00337623	IT Supplier Contractual Obligations Management, (undated)	POL-BSFF-0190525
439.	POL00337668	Post Office Limited IT Supplier Governance, November 2020	POL-BSFF-0190570
440.	POL00337628	IT Contract Management Governance & Operating Model, 2023-24	POL-BSFF-0190530
441.	POL00337625	IT Contract Vendor Management Team Maintaining a Supplier Relationship Matrix, (undated)	POL-BSFF-0190527
442.	POL00337633	Benefits Management Lifecycle, (undated)	POL-BSFF-0190535

WITN03680200

443.	POL00337637	Change Control & RAID or RIDAC, (undated)	POL-BSFF-0190539
444.	POL00337633	Benefits Management Lifecycle, (undated)	POL-BSFF-0190535
445.	POL00337634	Finance Process, (undated)	POL-BSFF-0190536
446.	POL00337640	Lessons Learned, (undated)	POL-BSFF-0190542
447.	POL00337630	Postmaster Engagement, (undated)	POL-BSFF-0190532
448.	POL00337641	All processes including Minimum Standards, (undated)	POL-BSFF-0190543
449.	POL00337635	Project Tasks and Milestones, (undated)	POL-BSFF-0190537
450.	POL00337638	Resource Management, (undated)	POL-BSFF-0190540
451.	POL00337631	Stakeholder Engagement - Engaging the Business, (undated)	POL-BSFF-0190533
452.	POL00337636	Status Reporting, (undated)	POL-BSFF-0190538
453.	POL00337639	Timecards, (undated)	POL-BSFF-0190541
454.	POL00337632	Tolerance Process, (undated)	POL-BSFF-0190534
455.	POL00362905	Cyber Security Standards, Acceptable Use Standard, 25 April 2023	POL-BSFF-0190850
456.	POL00362906	Cyber Security Standard, Access Control Standard, 25 April 2023	POL-BSFF-0190851
457.	POL00362907	Cyber Security Standard, Asset Management Standard, 25 April 2023	POL-BSFF-0190852
458.	POL00362908	Cyber Security Standard, Bring Your Own Device Standard, 25 April 2023	POL-BSFF-0190853
459.	POL00362894	Group Policy, Cyber and Information Security, March 2023	POL-BSFF-0190849
460.	POL00362909	Cyber Security Standards, Cyber and Information Security Standard, 25 April 2023	POL-BSFF-0190854
461.	POL00362761	Group Policies, Document Retention and Disposal Policy, 13 July 2020	POL-BSFF-0190846
462.	POL00362910	Cyber Security Standard, Encryption Standard, 25 April 2023	POL-BSFF-0190855
463.	POL00362911	Cyber Security Standard, Information Classification Standard, 25 April 2023	POL-BSFF-0190856
464.	POL00362912	IT Security Standard, Logging and Monitoring, 25 April 2023	POL-BSFF-0190857
465.	POL00362913	Cyber Security Guideline, Network Security Guideline, 25 April 2022	POL-BSFF-0190858
466.	POL00362914	Cyber Security Standard, Patch Management Standard, 25 April 2023	POL-BSFF-0190859
467.	POL00362919	IT Security, PCI DSS Compliance Guideline, 25 April 2023	POL-BSFF-0190864
468.	POL00362915	Cyber Security Standard, Penetration Testing and Vulnerability Scanning Standard, 25 April 2023	POL-BSFF-0190860
469.	POL00362916	IT Security Standards, Remote Access Standard, 25 April 2023	POL-BSFF-0190861
470.	POL00362828	Cyber Security Guideline, Secure Development Life Cycle (SDLC) Guideline, 02 August 2021	POL-BSFF-0190847
471.	POL00362917	Cyber Security Guideline, Secure Configuration Guideline, 25 April 2023	POL-BSFF-0190862

WITN03680200

472.	POL00362829	Post Office, Supplier Code of Conduct, 2022	POL-BSFF-0190848
473.	POL00362918	Cyber Security Standard, Vulnerability Standard, 25 April 2023	POL-BSFF-0190863
474.	POL00337657	EUC Managed Services, Service Specification Document, (undated)	POL-BSFF-0190559
475.	POL00337572	IT Change Management Process, (undated)	POL-BSFF-0190474
476.	POL00337596	Post Office Horizon IT, Defects Management Process, 31 August 2022	POL-BSFF-0190498
477.	POL00337652	Horizon Data Change Process, May 2021	POL-BSFF-0190554
478.	POL00337654	Introduction to the Post Office Horizon Release Management, January 2022	POL-BSFF-0190556
479.	POL00337651	Horizon Support Approval Process, 14 February 2022	POL-BSFF-0190553
480.	POL00337561	IT Policies, IT Change Management, 24 October 2018	POL-BSFF-0190463
481.	POL00337656	HNGA Release and Compliance Baselines, 24 September 2018	POL-BSFF-0190558
482.	POL00337650	Post Office Limited, Programme Test Strategy, (undated)	POL-BSFF-0190552
483.	POL00337662	Operational Working Agreement, 25 October 2021	POL-BSFF-0190564
484.	POL00337576	Problem Management, Process Overview, September 2023	POL-BSFF-0190478
485.	POL00337655	Release Management - For Service Transition and Operational Release, August 2023	POL-BSFF-0190557
486.	POL00337653	HM IT Release Management Process (Branch Counters), (undated)	POL-BSFF-0190555
487.	POL00337660	SD&T Process High Level, 30 August 2022	POL-BSFF-0190562
488.	POL00337661	IT Service Design and Transition Policy, 13 May 2019	POL-BSFF-0190563
489.	POL00337621	Capability Statement, (undated)	POL-BSFF-0190523
490.	POL00337567	Penetration Testing, Management Report, 21 November 2022	POL-BSFF-0190469
491.	POL00337568	Penetration Testing, Technical Report, 21 November 2022	POL-BSFF-0190470
492.	POL00337699	Global User Review, 2022	POL-BSFF-0190601
493.	POL00337700	Global User Review, 2023	POL-BSFF-0190602
494.	POL00337569	Description of Fujitsu's System of IT Infrastructure Services Supporting Post Office Limited's HNG-X Application, 1 April 2022 to 31 December 2022	POL-BSFF-0190471