UKGI00018115

Strictly Confidential

POST OFFICE LTD BOARD

Post Office Technology
Risk and Resilience Review

1. Purpose

The purpose of this paper is to update the Board on the findings and activities being taken in response to the recently commissioned KPMG Risk and Resilience report.

2. Background/Key Findings

2.1 Over the past 12 months our counter capability has experienced five major incidents. As part of the response Post Office commissioned KPMG to investigate our overall IT service landscape with a review of the current risk and resiliency of our services.

2.2 The review was wide and covered all Post Office services; however the assignment focused primarily on those with the potential for greatest impact on business and reputation.

2.3 Horizon received the greatest focus due to the critical nature of the service and its high public profile. Availability of Horizon Data Centre is critical as when unavailable the branch counter is unable to transact business.

2.4 The investigation was time boxed to one month to provide greatest benefit and responsiveness.

2.5 We have reviewed our IT roadmap and propose that as part of IT Transformation programme we will establish the business requirements, appetite for risk and associated costs to enhance our service availability. Implementation of any changes to our service availability would form part of our new IT Supply Chain and through the procurement of our IT Towers and Service Integrator.

2.6 Re-confirming with Post Office business stakeholders their expected business service levels over the 12-15 strategic period is being undertaken as part of our Towers procurement. This drives requirements and planning for:

2.6.1 Future Disaster Recovery and Systems Resilience capabilities which are being integrated into our IT procurement and refresh activities

2.6.2 Articulating the acceptable level of risk for the business

2.6.3 Accommodating essential improvements, with strong cost benefit cases, into the roadmaps for our legacy systems.

2.7 In the future, our chosen Services Integrator will as part of its BAU activities:

2.7.1 Undertake an annual Risk & Resilience review focussing on changes made and new areas of interest.

2.7.2 Ensure and maintain the readiness of our disaster recovery capabilities through amongst other activities scheduled testing.

3. Resilience Terminology

The terminology commonly used in considering the level of resilience of systems are detailed in the attached Annex.

UKGI00018115

4. Horizon Review Findings

4.1 Horizon's centralised Data Centre has resilience similarities with major UK organisations.

4.1.1 Retail

Retailers are focussed on the ability to continue trading even when their central Data Centre is unavailable. Retail POS systems are designed to continue to trade irrespective of Data Centre availability.

4.1.2 Banking

The Horizon Data Centre offers a lower level of resilience than those commonly found in the Banking sector.

4.2 The original Horizon system prior to HNG-x being implemented could transact non-banking functions without the Data Centre being available, similar to current retail systems.

4.3 Post & Go and ATM's will continue to offer customer service irrespective of Horizon Data Centre availability.

4.4 Whilst Post & Go can continue to trade end of day reconciliation would be affected as these transactions are reconciled via systems operated from the Horizon Data Centre.

4.5 Branches additionally have manual business continuity procedures for mails service (e.g. manual sale of stamps).

4.6 Horizon operates out of two physically separate data centres (Primary and Secondary) both located in Northern Ireland.

4.7 The Horizon Data Centre hosts multiple systems; the Horizon Counter Application, POLSAP[1], Credence[2], Post Office Data Gateway[3] and others.

4.8 As part of the renegotiation of Horizon in 2006 Fujitsu were contracted to manually recover the system to the secondary Data Centre in the event of a ("disaster") catastrophic event.

4.9 When not being used for a disaster situation the facilities of the secondary Data Centre are used to support testing of business changes requested by Post Office Ltd. This ensures we maximise value from our contracted assets.

4.10 Data Centre Failover

4.10.1 Any data centre failover event is operationally disruptive.

4.10.2 The Horizon business continuity plan identifies circa 70 events which will effect a failover.

4.10.3 Failover is an "all or nothing" activity.

---

[1] POLSAP: Provides support for finance.

[2] CREDENCE: Data Warehouse which is also used in the settlement of 3rd party Client and Agent remuneration.

[3] Post Office Data Gateway: Used to securely transfer settlement and other information between Post Office and 3rd Party clients (e.g. EON, AXA, Aviva, etc).

UKGI00018115

4.10.4 Currently all business services provided by the Data Centre must be failed over at the same time. (i.e. Horizon, POLSAP, Credence, Post Office Data Gateway, etc would all need to failed over together should any one require failover).

4.11 From the point of the decision to invoke disaster recovery (not the start of the incident) Fujitsu have to meet the following service level targets as agreed in the contract:

4.11.1 Restore counter banking services on Horizon within 2 hours

4.11.2 Restore all other Horizon services e.g. remainder of the counter services, web and Automated Payment Out-payment (APOP[4]) within 5 hours

4.11.3 Restore all other non-Horizon services e.g. POLSAP and Credence within 48 hours.

4.12 The currently contracted Horizon service availability target of 99.56% accepts that an average of two or three major service failures or 12 hours lost service time may occur per year.

4.13 Two out of the five Horizon service outages over the past twelve months were related to process rather than technical resilience.

Date	Incident	Cause
27/07/2011	PIN Pad transactions were unavailable between 08:00 and 14:30.	Reference Data delivery
12/12/2011	Banking Transactions were unavailable between 12:54 and 14:30.	Hardware failure
01/02/2012	Post Office Card Account (POca) transactions were unable to complete. In some branches Automated Payments (e.g. utility bill payments), E Top Up and a small number of Banking transactions were also affected. The service was impacted between 08:00 and 11:15.	Release Management process failure
01/03/2012	95% of transactions were unable to complete between 11:00 and 14:30.	Hardware failure
16/07/2012	Full service failure for 11 minutes, followed by a partial service for the next 35 minutes as the network restored itself. This was a result of a hardware failure within a network router switch.	Hardware failure

4.14 Only the incident on 12/12/2011 may have been preventable through additional investment in technology, or the move to an automatic failover.

4.15 While the architecture is generally designed for resilience, cost/risk trade-offs were agreed in the move from the original Horizon system to the new HNG-x one which mean that the service is not truly high availability.

[4] APOP (Automated Payment Out-Payment): a service provided by Horizon to enable various products to be sold and paid out from Post Office counters, on the instruction of our commercial clients (e.g. Postal Orders, NS&I, Payout, Stock Order, Bureau Pre-Order, Camelot Cheques, etc.).

UKGI00018115

4.16 Following the tactical review during April/May a programme of activities was undertaken to address improvements in infrastructure resilience, process robustness and service monitoring. All key actions have been completed, the remainder either require major release windows and have been scheduled, or are in the process of being prioritised with Post Office. On-going actions are being monitored through the joint Service Improvement Plan.

4.17 The latest incident has benefitted from the tactical changes made in response to previous outages, with Fujitsu being able to find and respond more quickly to the network incident on 16th July 2012 therefore reducing the overall business impact.

4.18 Moving to banking service levels within the current Data Centre capability (99.99% equating to circa 50 minutes service loss per year), was estimated by KPMG to require investment in excess of £50-70m[5] with a subsequent increased on going operational costs.

4.19 Channel Integration challenges the current risk/resilience profile as it increases the number of business services dependent on the Horizon architecture. The proposed architecture is currently being reviewed to ensure no degradation of the overall risk/resilience profile.

5. Web Findings

5.1 Post Office current web capability is provided through services contracted by Royal Mail Group with Capgemini and provided under the MSA agreed this year.

5.2 In the allotted time our consultants were unable to directly engage with Capgemini due to Royal Mail Group operational priorities.

5.3 The currently contracted service availability target of 98% accepts up to 170 hours of lost service time per year.

5.4 Although the Post Office Website does have a disaster recovery service in place, it is believed that this has limited capacity. In the event of a failover to the disaster recovery site it is not understood whether this would be adequate for POL's business requirements.

5.5 Any downtime is visible and also costly due to the number of high value financial services which are transacted though this channel.

5.6 We are continuing to engage with Royal Mail Group to understand the full capabilities of the Capgemini solution and expect to be able to provide an updated report at the beginning of October 2012.

5.7 As part of our separation activities we are working to determine the current and future business availability requirements which will be included in our future IT Supply Chain procurements.

The Board is asked to note the contents of the paper.

Lesley Sewell
September 2012

[5] Estimate by KPMG using industry standard Data Centre cost measures. These include Kw (kilowatt) power consumption, unit storage costs (per Terabyte), based on their experience of similar industry Data Centres. These figures do not include upgrade costs for hardware which might become end of life before the end of March 2015.

UKGI00018115

Appendix

Terminology:

Terminology	Description
Active / Standby	• Describes a model where the primary data centre runs the service and a second data centre is available to manually move the service to in the event of a disaster. • The Post Office system provided by Fujitsu Services Ltd currently adopts this model.
Active / Active	• Describes a model where both data centres are active at the same time. Whilst normally the business transactions run on the primary Data centre the second data centre is kept up to date (typically a few minutes). • Should the primary data centre fail the business load would be automatically switch (no manual intervention) to the second data centre. This would occur immediately with minimal or no perceived loss of service.
Disaster Recovery (DR):	• Typically occurs following a catastrophic event at the primary Data Centre and it is deemed necessary to fallback to a second site. Examples typically include flood, civil disturbance or other "acts of God". • This is a major event and our currently contracted levels for Horizon are typical in the industry. See below for contracted service levels.
Systems Resilience	• Redundancy built into systems to ensure that the system continues to run in the event of hardware or software failures. • Whilst these are significant events in their own right the system would be expected to continue to run at the primary Data Centre. Examples may be single server or disk failures.