IN CONFIDENCE

Report No: 68/01

Issued: January 2001

REVIEW OF HORIZON DATA CENTRES

ICL LTD

NOVEMBER 2001

REPORT DISTRIBUTION

For Information:	Mike Hannon	Horizon Contract and Commercial Manager
	Dave Miller	Managing Director Post office Network
	Paul Rich	Group Managing Director Post Office Ltd
	Peter Corbett	Finance Director Post Office Ltd
	Vince Mulholland	Head of Corporate and Strategic Finance Post Office Limited
	David Lewington	Head of Group Internal Audit
	Ernst & Young	External Auditors
From:	Rashpal Dhesi	Principal Auditor

Group Internal Audit
Consignia, AT21
Rowland Hill House
Chesterfield
S49 1HQ

Telephone: GRO
Postline: GRO
Fax No: GRO

INTRODUCTION

1.1 This report has been provided for information and summarises the detailed report produced by the International Computers Limited (ICL) Pathway Quality and Audit Manager covering the Horizon operations carried out at the ICL Data Centres based at Bootle and Wigan. The Horizon system records transactions carried out over the counter at Post Offices. The provision and management of the Horizon system for Consignia is carried out by ICL Pathway, who in turn have the Data Centres managed by ICL's Infrastructure Services Division (ISD). Under the contractual relationship, the recommendations made are the responsibility of ICL ISD to deploy.

1.2 As a result of a problem in retrieving archived data from the Data Centres, Consignia Group Internal Audit (GIA) asked to be involved with this review to provide assurance that problems relating to retrieval of archived data had been resolved. Although, the same data was archived at both sites, on one occasion, a tape holding the data was found to be corrupt, whilst the other tape was lost in transit by an external carrier. The data was eventually re-created using another source and no further issues have emerged.

1.2 The review also covered computer operations carried out from Belfast, but this was excluded from the GIA's remit as Horizon was only a small part of the total Belfast operations. The areas covered by the review were designed to assess the controls in operation over:

- firewall management;
- cryptographic key handling;
- physical security and logical security;
- management of backup procedures and media; and
- network management.

1.4 The main findings have been reported to the management of ICL ISD for action. The ICL Pathway Quality and Audit Manager will monitor progress of the deployment of these recommendations on a monthly basis. GIA will discuss progress made with the ICL Pathway Quality and Audit Manager at their quarterly meetings.

FINDINGS

Firewall Management

2.1 A firewall was used to regulate the flow of network traffic into and out of the Horizon network, using rules which were defined by the Data Centre. The product being used by ICL

ISD was called Firewall 1 which is a commercial package that has been developed by Checkpoint. The rules used by the firewalls have developed over time, but there is no complete audit log of the changes made to it. Recently, references relating to the firewall changes had been included in the change control process. No central review had been carried out of the firewall since its installation. Although security violations should be escalated to the Pathway Security Manager, firewall exceptions had not been defined leaving Data Centre staff unsure as to what would constitute a violation.

2.1 *The following actions had been recommended by ICL Pathway to their management, that*

- *a design specification is developed for the firewall rule base that establishes the optimum approach for defining and maintaining the rule base;*
- *the date and identity of the operator updating the firewall rule is included on the change log;*
- *the current firewall rule base is reviewed for completeness and accuracy by the ICL Pathway Security Manager;*
- *the ICL Pathway Security Manager provides clear guidance on what constitutes a security violation.*

2.2 It was also noted that it was possible to monitor traffic passing through the firewall, but this was being used to assist in bug fixing or monitoring traffic across a specific link. There was no active monitoring of attempted firewall breaches or other inappropriate activity across the firewall. Although active intrusion detection was available in the current product it was not part of the existing agreement between ICL Pathway and ICL ISD. *It has been recommended by ICL Audit that the ICL Pathway Security Manager reviews the position with regard to proactive intruder detection on the firewall and if considered necessary initiate changes to the relevant agreements between ICL ISD and ICL Pathway.*

Cryptograhic Key Handling

2.4 Data transmitted on the network was encrypted by the use of two keys (the Key Encryption Key (KEK) and the Data Encryption Key (DEK)) which were used to program the routers. There were a number of areas where local practices had evolved to meet local requirements and these were not consistent with the centrally produced procedures. These included:

- providing the duty manager access to the encryption keys as a matter of course (only the key custodian or deputy key custodian should have access);

- new local forms had been introduced in June 2001 to simplify the tracking of keys which were different to the current procedures;

- the new forms had been completed inconsistently and on some occasions in pencil.

Recommendations by ICL Audit have been made for the ICL Pathway Security Manager to review the above arrangements and either where the new processes are found to be adequate amend the procedures to reflect this or if inadequate enforce existing procedures.

2.1 The ICL procedures require that all cryptographic key material is segregated from other materials either through a separate safe or by some other form of separation in the same safe. The non Zergo crypto keys were not segregated within the main safe, and there was no separate safe for Zergo keys resulting in both sets of keys being stored together. *It has been recommended by ICL Audit that the ICL Pathway Security Manager review the adequacy of storing keys in this way and either change procedures to reflect current practice or to mandate the existing procedures.*

Physical and Logical Security

2.6 Both Data Centres are located inside existing Alliance and Leicester premises and to an extent the general security requirements of those organisations apply to the ICL ISD staff working there. The physical barriers, perimeter fence, road barriers, secured door, security guard, visitor log and passes, airlocks and proximity passes to access ICL areas, were all found to be working as expected. Visitors were escorted whilst on the premises.

2.5 A log of ICL visitor passes was maintained as well as copies of the passes issued. It was noted that passes can be made out in advance and if not used left in the log. *It has been recommended by ICL Audit that this practice stops and any unused passes marked 'NOT USED' and destroyed - a record being retained on the second copy of the pass.*

Management of Backup Procedures and Media

2.8 Off-site storage of back-up tapes was provided by Iron Mountain (IM), but managed by Belfast through the production of a daily schedule of back-up tapes to be collected and returned. IM provided strong boxes for the transport of these back-up tapes, and on collection, a local form was signed by the driver. There was no record of receipt from IM. On occasion there had been a discrepancy between tapes returned and what was due to be returned. *Hence, it has been recommended by ICL Audit that IM provide a receipt for tapes/packages taken into their custody. This could be delivered back to the Data Centres* *with the next set of tapes being returned.*

2.6 Special emphasis was placed on the handling and management of Data Tapes at the Data Centres following recent problems with the broken audit trail and difficulties at Wigan. A placement audit of the Data Tapes at the Bootle tape drives showed that they were positioned in accordance with the layout plan.

Network Management

2.10 The Data Centres continually monitor the state and status of the Horizon network using the Hewlett Packard (HP) Openview product. This system provides an audible warning if a link is lost and a visible notification as a new item appears on the network. There was no verification of the new item before an Internet Protocol (IP) address was allocated to it by the network team. Hence, there is a risk that rogue items could be connected and accepted into the Horizon network without check. *It has been recommended by ICL Audit that the network team introduce checks to verify new items before accepting them into the Horizon network.*

Agreed Action

2.11 GIA have agreed to monitor progress with deployment of the recommendations at the quarterly meetings held with the ICL Pathway Quality and Audit Manager.