POL00394026

Document Title:	Audit of Horizon Data Centres and Belfast Operations Centre
Document Type:	Report
Release:	N/A
Abstract:	This document presents the results of a planned audit into the activities and operation of the Horizon Data Centres at Wigan and Bootle and the Operations Centre in Belfast.
Document Status:	APPROVED
Originator & Dept:	J. Holmes (Quality & Audit) G. Hooper (Security) M.Ascot (IPDU)
Contributors:	
Reviewed By:	P. Jeram, M. Riddell, M. Stewart, C. Johnson (ISD), S. Gardiner (ISD), P. Sandison (ISD), A. Gibson (ISD)
Comments By:	
Comments To:	Originator (& Pathway Document Controller)
Distribution:	ICL Pathway Document Management, S. Muchow, P. Jeram, M. Riddell, M. Stewart, G. Hooper, C. Johnson (ISD), S. Gardiner (ISD), P. Sandison (ISD), A. Gibson (ISD)

POL00394026

0 Document control

0.1 Document history

Version	Date	Reason
0.1	12/11/01	First internal draft for comments
0.2	19/11/01	Following review cycle
2.0	21/11/01	For Approval

0.2 Approval authorities

Name	Position	Signature	Date
P. Jeram	Programme Director		
M. Riddell	Customer Service Director		

0.3 Associated documents

	Reference	Vers	Date	Title	Source

0.4 Abbreviations

Acronym	Meaning
ACP	Access Control Policy
BDC	Bootle Data Centre
BOC	Belfast Operations Centre
CGIA	Consignia Group Internal Audit
CKC	Cryptographic Key Custodian
CS	ICL Pathway Customer Service
DEK	Data Encryption Key
IPDU	Infrastructure Products Delivery Unit
ISD	Infrastructure Services Division
KEK	Key Encryption Key
SFS	Security Functional Specification
UKSS	United Kingdom Support Services
WDC	Wigan Data Centre

POL00394026

0.5 Table of content

POL00394026

POL00394026

1 Introduction

The Belfast Operations Centre is a vital part of the Horizon solution. It is responsible for the operational management of the Sequent and other systems at the Pathway Data Centres at Wigan and Bootle. It is also responsible for application support on Sequent and for Network Management that is undertaken at the Pathway Data Centres. Both Data Centres and the Belfast Operations Centre are managed by ICL's Infrastructure Services Division (ISD) on behalf of ICL Pathway.

2 Scope & Conduct

The audit was split into three elements. The first was to look at the operations and activities of the Data Centres at Wigan and Bootle and to consider the controls in place their against a number of pre-defined criteria, including firewall management, cryptographic key handling and physical security. The second was to look at the Operations Centre at Belfast where much of the work carried out at the Data Centres is controlled. The third was a configuration audit of a number of the live servers at the Data Centres to provide assurances on the state of the platform builds.

This report is a distillation of a number of Working Papers describing what was found and recording the various activities of the locations. It is not the intention to present the full extent of that information here, more the opinions and findings of the audit. If readers require access to the background material it can be made available through the ICL Pathway Quality & Audit Manager.

The scope of the audit was defined in formal Terms of Reference, issued by Pathway IA in October 2001 and presented at Annex A to this report. It is part of the ICL Pathway Internal Audit Plan for 2001 and while it was primarily interested in the applications and effectiveness of controls it also took into account the requirements of ISO9001:2000 and ISO17799:1998.

The audit was conducted during October 2001 by Jan Holmes (Quality and Audit Manager), Graham Hooper (Security Manager) and Mark Ascot (IPDU), all from ICL Pathway. Rashpal Dhesi from Consignia Group Internal Audit attended the Wigan and Bootle elements of this audit as an observer.

The help and co-operation of all members of ISD staff interviewed is appreciated.

POL00394026

3 Management Summary

3.1 Data Centres

Although there are a lot of recommendations presented for the Data Centres, the overall opinion is that the management and operations at Wigan and Bootle are sound and under control.

Scrutiny of the recommendations indicates that a number are linked to the over arching Pathway Process RS/PRO/036. This process must be reviewed and updated to reflect local practice (KEK & DEK control forms), which was considered to be good, and the issues around physical segregation of Keys in the main safes where a ruling from the Pathway Security Manager may be required. (See 4.4 and 4.13)

The lack of personnel security vetting, as required in RS/PRO/002, must be addressed, particularly as this process was introduced following a recommendation made in an earlier audit. (See 4.5).

The Firewall was being managed effectively although the underlying basis for the Firewall rules is evolutionary and no real baseline has ever been established. An audit of the Firewall rule base, followed by the production of a specification, the continued application of the strong controls already in place, and recommended improvements, should remove any uncertainty about the integrity provided by this product. (See 4.14).

There is concern about the break in control between allocating an IP address v**ia OCP** to a new terminal and then accepting it into the Network but a simple check, followed by an update to the IP database, could remove that weakness. (See 4.15).

The arrangements with Iron Mountain require a review, in particular the staff vetting procedures and the receipting of tapes and material sent there for storage. (See 4.16).

3.2 Operations Centre

Although there are a lot of recommendations presented the overall opinion is that the management and operations at the Belfast Operations Centre are sound and under control. Most of the recommendations are pertinent to a few specific areas and non-compliance is generally the result of staff having to undertake operational support on a complex architectural environment for which the approved methods of administration are no longer sufficiently effective.

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.

POL00394026

User account administration should be reviewed and enforced to obviate the need to by-pass approved account policies by using Administrator privilege.

Secondary authentication procedures would benefit from review in conjunction with CS Security

A number of extant operational security procedures need to be documented and enforced.

The handling of cryptographic keys needs to be reflected within central Pathway procedures.

The failure of a number of key processes is contributing to difficulties in identifying and assuring the correct state of various live platform builds.

4 Detailed Observations

4.1 Organisation and Structure

Both Data Centres and the Belfast Operations Centre (BOC) operate within an established organisational structure with clear line management and escalation routes. This is particularly important at BOC where Pathway is not the only ISD customer supported from that site.

At the BOC activities are segregated into discrete functional areas (DBA, Pathway UNIX, Systems Management/Home Services UNIX and NT). DBA, Pathway UNIX and Systems Management functions are dedicated to Pathway operations whilst NT support is shared between Pathway and other ISD supported areas.

Designated Managers are responsible for each functional area and the Head of Pathway UNIX is dedicated as the lead managerial contact. Pathway's primary interface with BOC is via the ISD Pathway Operations Manager based at IRE11 and the Pathway CS Service Manager based at BRA01. Senior ISD Line Management at Belfast is also responsible for ISD GIO operations at the Wigan and Bootle Pathway Data Centres.

At the Data Centres the split is essentially between Network Management and Operations staff. Each site has a nominated Data Centre Manager and a Duty Manager function operates **during the day shifts with technical on-call out of hours, though the DCs are manned 24/7.**

4.2 Policy, Contractual and other Security Requirements (Belfast)

Baseline Information Security Requirements are driven largely by ICL Group (GISI) policy. This mandates the use of ISO17799 as the approved standard by which information security is established and maintained. This is evidenced by Corporate Policy Framework relating to Security. These policies are supported by legal and general contractual obligations to other customers and best practice from these is utilised within other contracts including

POL00394026

Pathway. BOC do not undertake additional internal reviews outside the requirements placed upon them by ICL Group.

The general security ethos within BOC is well established and permeates the operation at IRE11.

BOC believe that they are required to support the requirements of Pathway specific Contract Controlled Documents (CCDs) primarily the Security Policy (RS/POL/002) and the Security Functional Specification (RS/FSP/001). Also of relevance is the Access Control Policy (RS/POL/003). There is some doubt however within BOC that the contract between Pathway and ISD formally reflects these requirements.

It is recommended that the Pathway Service Manager for ISD reviews the contract between Pathway and ISD to ensure that Pathway's contractual obligations are adequately reflected.

It is also recommended that extant versions of the SFS and ACP are issue to ISD for formal review.

4.3 Physical Security

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 ISD staff working there. The approach here was to look at physical security as a set of layered controls from barriers external to the buildings to the use of tokens to control movement and access internally.

4.3.1 Data Centres

The physical barriers in place at Wigan, perimeter fence, road barriers, secured door, Security Guard, visitor log and passes, airlocks and proximity passes for access to the ICL parts of the building, were all found to be working as expected. Visitors are escorted and an attempt to use a visitor proximity pass to obtain access to the external building doors failed.

A log of ICL visitor passes is maintained and copies of passes issued retained. It was noted that passes can be made out in advance of visits and if not used left in the log.

It is recommended that this practice is stopped and any unused passed marked as 'NOT USED' and destroyed – the record is retained on the second copy of the pass.

POL00394026

The workspace is mixed with A&L staff but there is sufficient segregation between the two groups, including inside the Computer Room, to ensure the safety and integrity of ICL's activities there.

As with Wigan the physical barriers were exercised in order to gain access to the ICL part of the building and, as with Wigan, were all found to be working as expected.

However, it was noted that the main exit gate for this site was permanently open allowing unrestricted access. This compromises what is otherwise a strong regime.

Both Bootle and Wigan Data Centres are located on Alliance & Leicester sites and are subject to elements of A&L's security, Health and Safety and fire requirements. A&L's Property Manager was able to confirm that following some problems in the early days there had not been any 'difficulties' or security issues around the ISD tenancy. He also confirmed that a Wigan Tenants Group had been established and had met a couple of times. Unfortunately ISD had not been able to attend either one and it was stated that the meetings often dealt with low level A&L site management and personnel issues. However, there may be occasions when it is appropriate for ISD to be represented and they should endeavour to attend Tenants meetings at these times.

4.3.2 Operations Centre

Physical security at IRE11 is extensive and commensurate with the prevailing threat. The site is contained within a well-defined and secure perimeter that is adequately fenced and monitored via CCTV with infrared capability. Access to the site is via a single entrance point for both vehicles and pedestrians. This is adjacent to a gatehouse that it manned on a 24-hour basis. All visitors are subject to bag-search at this point.

Within the perimeter there are separate buildings for the administrative and data-centre operations. The car park is located some distance from both buildings and visitor's vehicles are allocated parking bays furthest away from the buildings.

The administrative building has a reception point and all visitors are required to sign in and be escorted at all times. Intruder detection operates within the building and access to areas is controlled by proximity pass. Pass control and the guard force is administered by Chesterton Workplace Management under contract to ICL. Allocation of passes is permitted only when security vetting procedures have been successfully completed and all leavers are removed immediately from the system.

The Data Centre building is protected by an additional perimeter fence. Access to the building is via proximity pass that permits access only to those personnel that require access. Internal proximity detectors are configured to provide further granular segregation so as to restrict access to specific areas within the Data Centre – most noticeably to the machine room. Intruder detection also operates within the Data Centre.

POL00394026

No issues were identified or reported and it is considered that the physical security, fire and Health and Safety arrangements at IRE11 meet or exceed requirements.

4.4 Data Centre Safes

This is a specific section in the report as the provision and use of a main safe at the Data Centres is vital to maintaining the security and integrity of the Horizon solution. Central to this are the cryptographic keys used to encrypt the hardware and networks, and the controls exercised over them by Data Centre staff.

There are two safes at Wigan, The main safe is located in the Computer Room an contains a variety of items. Of these, the key items are the non-Zergo cryptographic keys and control documentation, the visitors day passes, the crypto transfer safe and the CCTV recording tapes. Other important documents and items are also held within the safe.

An inventory of the safe is maintained and checked on a monthly basis although records only go back as far as August 2001. A simple tick is used to indicate the presence of an item and this is not sufficient to identify when the check as made and by whom.

It is recommended that the inventory check is dated and the checklist to be signed by the person making the check to indicate the presence of items. A countersignature should be obtained upon completion of the check. This recommendation applies equally to Bootle where the same practice takes place.

RS/PRO/036

Note : All recommendations marked RS/PRO/036 will be dealt with as a single Corrective Action on the CAP.

The second safe is in the Control Room and this holds the Zergo cryptographic keys, swipes and control documentation.

These are key operated safes and normal access is granted to the Data Centre Site Manager (Paul Sandison), the Network Manager (Colin Johnston) and the Duty Manager (Tim Roper). Other access is by exception.

RS/PRO/036 requires that ALL cryptographic key material is segregated from other materials either through a separate safe or by some other form of separation in a shared safe. The non-Zergo crypto keys are not segregated within the main safe.

There is only one safe at Bootle and this is smaller than Wigan's. There is also no separate safe for Zergo keys resulting in both sets being stored together and not segregated from other material in the safe.

POL00394026

It is recommended that the requirements expressed in RS/PRO/036 regarding the separation and segregation of cryptographic key material from other sensitive material for storing in safes is reviewed by the Pathway Security Manager. Both sites currently fail to conform to the requirements of the process and a decision is required about continuing with the current arrangements and amending the process to reflect that, or to escalate the non-conformance and mandate the requirements. This recommendation applies equally to Wigan where the same problem exists.

RS/PRO/036

4.5 Personnel Security and Vetting

The audit of Customer Service in January 1999 identified that personnel security vetting was not taking place for Pathway employees. As a consequence RS/PRO/002 – Pathway Security Vetting Process was developed and published. The process is invoked by Pathway HR on notification that a new employee has joined the project, either directly through Pathway or via a key supplier such as ISD. The audit identified that no new members of the ISD teams at Wigan or Bootle have been subjected to a security vet for the last 2 years.

All personnel at IRE11 are required to successfully complete formal HMG vetting requirements that include police (CRO) and Security Service Counter Terrorist (CTC) checks. This level of vetting is more extensive than the baseline requirement mandated by Pathway.

Notwithstanding this there is an ongoing requirement to administer the approved Pathway vetting process. Whilst the BOC Admin reported that this should be operating correctly it was not possible during the audit to meet with HR and review implementation and compliance.

It is recommended that the Pathway Security Manager and Pathway HR review the operation of this process since it does not appear to have been successfully implemented.

It is recommended that ISD Personnel be asked to confirm that the process documented in RS/PRO/002 has appropriate visibility and is being complied with for recruits to ISD BOC.

POL00394026

4.6 Access Control and Account Administration (Belfast)

A fundamental security requirement is the segregation of duties relating to the administration of Unix and NT. The organisational structure of BOC reinforces this distinction and BOC users are allocated specific roles and responsibilities based upon the agreed requirements of the Pathway Access Control Policy.

In the main all users requiring Unix level access to the system access it via a secure menu system on an NT workstation. This constrains the functions called depending on the user's role and audits all functions performed by the user. Particular emphasis is placed on securing the role of System Administrator, which has access to powerful resources including root privilege, Unix commands and DBA functions.

It is noted that a decision was made following the initial release of Horizon not to enable Unix auditing, but to enable "C2" compliance in the Dynix kernel. At SIP14 Dynix was updated to version 4.4.4, which silently turned on auditing when "C2" was selected. This was found to conflict with the implementation of Metron Athene, and a Pathway decision was made to disable C2 compliance in the kernel. From a security perspective it is preferable to re-enable C2 in Dynix and a review of the impact on applications and support will need to be carried out.

The BOC DBA is responsible for the maintenance of user accounts for access to live systems. In the main this is controlled but there is evidence that redundant domains, user roles and users are not being removed from the system as is required by the SFS and ACP. This is in part due to non-reporting to BOC of Pathway leavers.

Procedures for authorising access to the live estate are documented in RS/PRO/040 and the process is considered to be effective. It was reported that additional information could be captured on the request form to ensure that the correct privileges are enabled. It is also apparent that the separate forms used for KMS-related access and general live estate access should be rationalised.

It is recommended that the process and activities surrounding access to the live estate is reviewed. This should include :

- *ISD undertaking a full review of the current user accounts with a view to correcting discrepancies.*
- *ICL Pathway Security reviewing the process for informing BOC of changes.*
- *ICP Pathway Security reinforcing with HR the need for regular monthly updates of leavers.*

POL00394026

- *ICL Pathway Security and ISD reviewing RS/PRO/040 to addressing these issues.*

The Root Administrator password for the live estate has recently been changed following a request by CS Security. This global password must however be changed at least quarterly to prevent unauthorised access to the live systems. This has not been implemented.

It is recommended that ISD develop and document a process for changing this password and ensure that it is applied by cross-referencing within the Duty Manager's Checklist.

4.7 Remote Administration (Belfast)

Systems are generally configured to reduce the risks of human users interfering with automated applications. Users accessing sensitive data at the Data Centres or updating any information use secure build workstations that are connected via the secure LAN. The corporate LAN is entirely separate. Workstations have floppy/CD drives disabled except where exceptions have been agreed. All users generally authenticate to the appropriate PWYDCS domain (but see below) via secondary (SecurID) token. There is evidence to indicate that SecurID is not enabled on some support workstations although they are configured with a 10-minute lockout.

It is recommended that SecurID be enabled on all workstations to comply with requirements of the SFS and ACP. This will require BOC to monitor the console sessions of the Firewall and ACE servers.

The SFS mandates the use of Tivoli Remote Console (TRC) for the remote administration of Data Centre platforms. This records an auditable trail of log-ins to all boxes accessed by the user. It is a matter of considerable discussion and correspondence that TRC is slow and difficult to administer. This has lead over time to BOC personnel relying heavily on the use of unauthorised tools (predominantly Rclient) to remotely administer the live estate. Its use is fundamental for the checking of errors. The tool does not however record individual user access to systems but simply record an event (2002 info, 2004 warning and 2006 info) on the remote box that Administrator access has been used. No other information is provided including success/fail so it is not possible to simply audit failures. Their use puts Pathway in contravention of contractual undertakings to Post Office. (See also Software Distribution and VNC).

POL00394026

It is recommended that Pathway APDU continues its work to establish an alternative support tool that facilitates the auditing of individual user access or creates a means by which the use of current tools can be similarly audited.

Where BOC staff need to access the PWYHQ domain they can only do so as Administrator. This is because PWYHQ and PWYDCS domains have been created as Master Domains and a trust relationship between the two cannot be established. There is also evidence of high usage of access to systems via PWYDCS using root Admin privilege.

It is recommended that the domain structure be reviewed by ICL Pathway Security with a view to establishing a domain architecture that allows access with least privilege.

It is also recommended that User Account processes are reviewed to obviate the need for access using Administrator privileges. This applies equally to NT and Unix.

4.8 Storage and the use of Sensitive Information (Belfast)

Designated BOC staff have access to a fire-safe held in the Technical Support office. This is used primarily used to store passwords under cover of sealed and signed envelopes. This includes Unix root and NT Global Admin passwords. The safe is also used for non-Pathway related storage.

It is recommended that a discrete safe is obtained and used for Pathway related information. Alternatively a smaller secondary safe should be provided within the main safe to which only BOC personnel supporting the Horizon system should have access.

RS/PRO/036

Few sensitive documents or data are held by BOC and all information is handled within the secure operations area. BOC would however benefit from the provision of additional, lockable cabinets to remove paperwork from the operational environment.

POL00394026

4.9 SecureID Administration (Belfast)

The recent new ACE/Solaris secure build has caused problems because the Console Buffer on the Terminal Server is filling, resulting in the system hanging until a console connection is established in Belfast. This is also true of the firewall build, and has led to the practice of leaving console sessions on these platforms open in Belfast. Whilst these are in a secure area, this effectively gives unmonitored physical access to the platforms.

User accounts are being locked out because the security model assumes users connect frequently, whereas for these platforms the need to connect is rare, when a user is on call and there is a problem. The only solution is to force a logon through anonymous root privilege, which bypasses agreed security procedures. It is understood that a fix has been developed but has yet to be released.

It is recommended that Release Management arrange for testing and delivery of this fix so that SecurID administration can be performed in accordance with agreed policy.

The current process documented in RS/MAN010 for SecurID token Administration can delay the time necessary to remove users from the system.

It is recommended that RS/MAN/010 is reviewed to consider the disabling of the token by CS Security when a user leaves prior to sending a system-disabling request to BOC.

4.10 Event Handling (Belfast)

An extensive event handling system is managed by BOC utilising approved tools BMC Patrol is run on the Unix hosts and HP Openview is used to monitor networks at the Data Centres. Maestro Scheduler raises specific events and system events are also forwarded via Tivoli.

Event filtering is undertaken by the use of KELs a recent review of which substantially improved the handling of events.

For systems monitoring purposes Insight Manager is used to hook into the BTI system and forward alerts direct to the Duty Manager.

POL00394026

4.11 Software Distribution, Installation and Platform Builds (Belfast)

Tivoli Courier is the approved method of distributing and installing software and patches to the live estate. This has proven unreliable and slow in the majority of cases - particularly during major upgrades. The demands of accuracy and expediency have forced the use of VNC, which is now used extensively for installing patches and applying release notes to live. The use of this product runs contrary to Pathway policy because it does not audit individual access to the system or the changes made. This difficulty is compounded because in the vast majority of cases, software packages require Domain Admin privileges.

It is recommended that Pathway APDU continues its work to establish an alternative software installation tool that facilitates the auditing of individual user access or creates a means by which the use of VNC can be similarly audited.

In the majority of cases software released from CM is sent to ISD via the CM Signing Server and from there to the ISD Staging Server. This is used to deliver software to the .26 Rig and is also accessed by ISD via an appropriate share. ISD report however that they have no way of proving the integrity of packages originating accessed via SYSDEL01.

It is recommended that this process be reviewed to determine whether it is appropriate to include a signature verification check on the Staging Server.

A recurring problem concerns the ability of Pathway to obtain assurance that the build state of live platforms, servers and workstations aligns with the respective baselines delivered by PIT and held by CM. A significant amount of historical evidence indicates that the build of live boxes is not representative of approved Pathway baselines or of the build on the various Test Rigs. The reasons for this may be manifold (e.g. a failure in the PinICL process to update baselines after an interim urgent OCP fix has been applied to live, a test workaround that has not been included in the Release Note, a failure by ISD to follow the script or a combination of these).

It is recommended that these various processes be reviewed. The vagaries of build states is a significant security risk that would affect the ability to recover functional platforms in the event of a disaster and potentially lead to release notes working in a test environment but failing in live.

POL00394026

A contributory factor is the lack of a test rig that is fully representative of live. Advances have been made recently in this area but consideration should be given to the possibility of combining the Release and .26 Rig for this purpose.

The use of the PIT "Fingerprint" .exe was also designed to provide assurance that the correct domain and platform were targeted for software upgrades and that release notes were applied in the correct order. Whilst this provides some assurance it does not validate the build nor indicate whom was responsible for applying it.

It is recommended that until a suitable method is devised for tracking Release Notes (i.e. via CM software), the Fingerprint script should include an event to indicate who applied the release note.

There is evidence that the initial password included in the PIT baseline is not being re-named prior to introduction to live. This is of significant security concern.

It is recommended that ISD develop procedures that ensure that the initial build password is re-named when platforms are commissioned to live service.

4.12 Cryptographic (Non-Zergo) Key Management

This particular aspect of the Data Centre's operations was not covered in sufficient depth to enable an opinion to be drawn.

It is recommended that the Pathway Security Manager conducts a review of non-Zergo key management at the earliest opportunity.

RS/PRO/036

4.13 Cryptographic (Zergo) Key Management

4.13.1 Data Centres

The requirements for these controls are defined in RS/PRO/036 v1.0 dated 12/06/00 available on the Pathway BMS and made available to ISD staff by the ICL Pathway Security Manager. This has in turn been interpreted and the ISD local procedure ICL/PW/NET/PRO/006 Zergo Operations Guide v4.0 dated 25/10/01 was seen.

POL00394026

Details for the safekeeping of Zergo keys on-site are described in para 4.2. The despatch of Keys to the Data Centres is controlled by the Pathway Security Manager. On receipt at Wigan the Data Centre Site Manager inspects the package for damage before opening and checks the content against the Despatch Note enclosed. It was noted that the Despatch Note refers to named links that do not reflect the real world link and this is a cause for confusion when identifying Keys for transfer.

It is recommended that the Pathway Security Manager review the Despatch Note link identities to remove any confusing link names and replace them with meaningful real-world identities.

RS/PRO/036

The Keys are sorted and those that are destined for Bootle identified and placed for safekeeping in the secure transfer box inside the main WDC safe. These are collected at some appropriate time by the Bootle Network Manager are transferred to Bootle and stored in the main BDC safe. (See recommendation in Para 4.4 regarding non-segregation of Key material in the main Data Centre safes).

Access to the safes, and therefore the Keys, is currently limited to the Key Custodian, the Deputy KC and the Duty Manager. This is contrary to RS/PRO/036 that describes access by the Duty Manager as an exceptional item and subject to extra control. It was suggested during the audit that restricting access to the KC and DKC only was restrictive and the addition of the Duty Manager is a necessity. This was subsequently confirmed during the report review cycle.

It is recommended that the Pathway Security Manager review the arrangements for access as part of the broader review of RS/PRO/036.

RS/PRO/036

The Keys are held as sets in a specially made plastic wallet such that the single KEK is associated with the physical key and the seven DEKs. A Local Key Inventory Form has been introduced that mirrors the physical position of the Keys in the wallet and provides details of receipt, use and destruction with a name and date associated with each state. The nature of the form makes it extremely easy to identify where a Key is missing and why.

This is a local initiative and was introduced in June 2001 to simplify the tracking of Keys. It does not conform to the requirements of RS/PRO/036 although it is an improvement on the control documentation prescribed.

POL00394026

Similarly there is a revised movement control form for Remote Keys and this was introduced at the same time. As with the Local Keys Inventory Form the new form is an improvement over that defined in RS/PRO/036.

It is recommended that RS/PRO/036 is reviewed and updated to reflect the use of the new inventory and movement forms.

RS/PRO/036

Unfortunately the improvements provided by the new forms is offset by the inconsistent completion of the fields and the use, on some occasions, of pencil.

It is recommended that the forms are reviewed at both locations for completeness, updated accordingly and that in future fields are completed using a pen or biro or other permanent marker.

RS/PRO/036

Finally, it was reported that some of the links for which Zergo encryption keys had initially been produced had since changed. As DEK and KEK keys are printed with details of the remote site locations this has potential for confusion.

It is recommended that the Pathway Security Manager and supplier review the key set and amend details to reflect the current requirements.

RS/PRO/036

4.13.2 Operations Centre

There is a designated Cryptographic Key Custodian (CKC) for BOC but this role is not currently recognised within extant documentation (RS/PRO/036). There is also no designated Deputy in the event that the Primary CKC is unavailable.

It is recommended that RS/PRO/036 be revised to incorporate this role and ISD identify a suitable deputy.

RS/PRO/036

The CKC is responsible for a small number of Key Encryption swipe cards that are used on the Zergo hardware encryption devices at IRE11 and IRE19.

POL00394026

All handling appears to be generally consistent with requirements but the keys themselves are stored (under sealed cover) in a safe to which unauthorised individuals have access. There is therefore the potential that keys could be compromised.

It is recommended that the CKC be provided with a separate safe for the storage of keys. Alternatively given the small number, keys should be stored in a separate lockable box within the main safe to which only the CKC or deputy has access.

RS/PRO/036

The CKC has copies of a number of cryptographic procedural manuals including the Zergo Operations Guide but not RS/PRO/036. A check of cryptographic records held by the CKC showed that whilst due diligence is being applied in the receipt, recording and maintenance of key related functions, as with the Data Centres, the documentation being used is not as defined in RS/PRO/036.

It is recommended that RS/PRO/036 be re-circulated for review to capture BOC requirements and revised to include standardised templates.

RS/PRO/036

4.13.3 Review and Audit

There is no regular independent review of this process, either by ISD or Pathway. While the audit has identified a number of minor issues at all locations that, if considered independently or collectively, do not represent a significant threat to the security and integrity of the network, nor is there any suggestion of accidental or deliberate malpractice within the Data Centres, the handling and management of the Keys is sufficiently important to warrant a regular review by ISD management, independent of those who operate the process.

It is recommended that ISD introduce a regular review of Key management activity at the Data Centres and Belfast. A six monthly cycle is suggested as being adequate.

It is also recommended that a review of Key management is conducted by ICL Pathway on an annual basis. This can be achieved as part of an annual audit of the Data and Operations Centres' activities.

POL00394026

4.14 Firewall Management

Firewall management is achieved through the implementation of the FireWall1 product from Checkpoint. The current rule base has developed over time and there is no 'specification' as such that established the original requirement. While the firewall has been updated over time it is not clear whether the most appropriate methods are being used. For example, new AP Clients are simply added on as a new rule rather than adding a new instance to an existing object group. A dedicated workstation exists at each location and in terms of coverage Wigan is responsible for the maintenance of the Wigan firewall while Bootle manages Bootle and all remote sites, eg. FEL01 and BRA01.

It is recommended that a design specification is developed for the Firewall rule base that establishes the optimum approach for defining and maintaining the rule base.

Changes are managed through the OCP process and evidence was obtained of one such change (OCP3364) at Wigan. There is no complete audit log of changes made to the firewall rule base although ISD have recently started to include the OCP reference against the firewall record where a change has been made but it is considered that this 'change log' would be enhanced if a date and operator identity can be identified alongside the OCP reference.

It is recommended that the identity of the operator updating the firewall rule base and the date of update is included in the 'change log' field of the database.

There has not been any central review or audit of the firewall rule base since its inception although the Pathway Security Manager has access to the current settings via a terminal in the Secure Room in FEL01 A0. The lack of regular review coupled with the historical evolution of the rule base could lead to incorrect or irregular entries and settings.

It is recommended that the current firewall rule base be audited for completeness and accuracy by the Pathway Security Manager and an ongoing programme of reviews established.

It is a requirement that security violations are escalated to the Pathway Security Manager. However, firewall exceptions have not been defined leaving Data Centre staff unsure what would constitute a violation should one exist.

POL00394026

It is recommended that the Pathway Security Manager provides clear guidance on what is a reportable security exception for the firewall.

It was noted that it is possible to monitor traffic passing through the firewall along a specific link although this is only used accommodate bug fixing or to monitor traffic across that link on demand. There is no active monitoring of attempted firewall breaches or other inappropriate activity across the firewall. It was stated that active intrusion detection is available in the current product but was not part of the existing agreement between Pathway and ISD.

It is recommended that the 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 ISD and Pathway.

4.15 Network Management

The Data Centres continually monitor the state and status of the Horizon network using the HP Openview product. Dedicated terminals exist at both locations and each has a complete view of the full network. Although access to the terminals is unrestricted within the Control Rooms it is members of the Network Team who are **solely** responsible for the active monitoring of the network. Audible warnings are provided by the system if a link is lost and a visible notification is an item appears on the network that has not been previously notified.

Additions and changes to the network are managed through the OCL process and evidence was obtained (OCP2373) for one such change at Wigan. Upon request the IP Database is accessed by Data Centre staff and a free IP address allocated to the terminal. Unlike the Firewall rule base there is no record on the IPDb of what initiated a change nor who made it and when it was done.

When a new item is attached to the network is it identified by the HP Openview and placed in a transit area on the screen. This is then associated to the appropriate part of the network by one of the Network Management team. There is no verification of the new item and the IP address is not checked against the IP Database. Before an IP address is allocated to a new terminal the addition would have to been approved through the OCP process and, if initiated by Pathway, the CP process. These are strong controls but they are compromised by the lack of verification of new items and there is a risk that rogue items could be connected and accepted into the Horizon network without check.

POL00394026

It is recommended that the IP Database spreadsheet is improved to include columns that identify the OCP number, operator identity and date for each new or changed IP address. It is also recommended that more effective checks be introduced to verify that new items identified on HP Openview are verified and authorised by Network Management before being accepted into the Horizon network. This could be achieved through a further column in the IP Database and the relevant Network Manager 'signing' against the IP address entry acknowledging that the terminal has been accepted into the Network.

POL00394026

4.16 Backups and Offsite Storage

Offsite storage is provided by Iron Mountain (IM), formally DataVault and is controlled by Belfast although exercised by the Data Centres. The schedule has been devised by Belfast who provide the Data Centres with a daily schedule of tapes to be delivered to and collected from IM. This information is transferred to a local form where any local additions are made and the tapes picked and packed into strong boxes provided by IM. The local form is faxed by the Data Centres to IM who pick the tapes for return and arranges for the transfer of tapes at the Centres. IM provide a delivery schedule with each load although they do not provide a corresponding receipt for tapes received from the Data Centres other than the driver signing the local form.

It is recommended that Iron Mountain be requested to 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.

The handling of off-site storage of back-up media for BOC is also undertaken by Iron Mountain. They provide secure facilities for the back-up storage of Dynix operating system, Database and Applications data. A considerable number of tapes and other media are entrusted to this company but it has been some time since a review was undertaken into the continued security of their operation.

It is recommended that a vetting review of Iron Mountain operations (storage arrangements, schedules, staff vetting etc.) is undertaken by ISD in order to provide continuing security assurance for assets entrusted to them.

4.17 Business Continuity

4.17.1 Data Centres

The requirement to provide effective Business Continuity is established by R830 of Schedule A15. The overall Business Continuity Framework, including that for the Data Centres, is owned and managed by Pathway Customer Service and is documented in CS/SIP/002 v5.0 dated 31/10/00. This identifies some 22 Business Continuity Plans covering a number of different technical areas of the Data Centres, including the physical campus itself, and these are regularly run by ISD on behalf of CS. A further key document is SU/MAN/018 the ISD Operational Procedures Manual Front-End Index. This identifies all current ISD operational procedures that must exist in order to ensure controlled and continued operations at the Data Centres and other ISD sites.

POL00394026

While CS/SIP/002 clearly identifies the existence of SU/MAN/018 there is no reciprocating identification from the ISD list up to the BC Framework. This is a very minor point but without the upward reference the importance of SU/MAN/018 in the overall Business Continuity Framework may be overlooked.

It is recommended that SU/MAN/018 be updated to include clear references to CS/SIP/002.

There is a scheduled series of Business Continuity tests that are co-ordinated by Pathway Customer Service in conjunction with ISD. ISD also undertake their own internal reviews of arrangements, the last such session being February 2001. A short report was prepared and a follow-up visit made approximately 6 months after the test. Copies of the report and follow-up notes were obtained during the audit. Local procedure ICL/PW/NET/PRO/012 v1.1 dated 13/09/00 Business Support Contingency Operations Guide describes this activity.

4.17.2 Operations Centre

The physical security arrangements in place at the IRE19 contingency site were reviewed during the audit.

The site at IRE19 is an inconspicuous building within which BOC has a designated area within which to conduct operational support for Horizon in the event of a failover. Adequate physical security is evident comprising perimeter fencing and CCTV. There is an on-site guard presence during the day, which ensures suitable reception arrangements for staff and occasional visitors. Regular failover / fallback tests are undertaken at the site.

Failover procedures are included in the operational procedures manual.

4.18 Operational Procedures

4.18.1 Data Centres

The opportunity was taken to review the existence and status of local procedures as topics were discussed during the audit. A number of local procedures were examined including :

ICL/PW/NET/PRO/006 v4.0 dated 25/10/01 – Zergo Operations Guide

ICL/PW/NET/PRO/010 v1.1 dated 05/01/01 – Remote Site Operations Guide

ICL/PW/NET/PRO/011 v1.6 dated 11/10/01 – Peripheral Operations Guide (W)

ICL/PW/NET/PRO/012 v1.1 dated 13/09/00 – Business Contingency Guide

POL00394026

There were clearly many more documented procedures available in binders positioned on the 'bridge' and available online on the DC Server. Procedures are subject to regular reviews and this is indicated by some of the dates and revision numbers of those seen. PRO/012 is probably due for a review being now some 13 months old.

Elsewhere in this report there is evidence of process improvements being made, in particular the local guidance for the handling and management of Zergo Key material, and this is commended.

Special emphasis was placed on the handling and management of DLTs at the Data centres following the recent problems with the broken audit trail and current difficulties at Wigan. A placement audit of the DLTs in the Bootle tape drives showed that DLTs were positioned in accordance with the layout plan provided by Richard Laking. Given the problems being experienced at Wigan the exercise was not repeated there.

4.18.2 Operations Centre

The operational procedures required by BOC to support the Pathway / Horizon infrastructure are consolidated into the ISD Pathway Operations Manual. ISD were not prepared to provide a copy of the manual at the time of the Audit on the basis that this was an internal ISD document. ISD did provide an overview of its content headings and format but it is difficult for Pathway to obtain assurance unless it has formal visibility of this document.

It is recommended that the Pathway CS Service Manager (Mike Stewart) has access to this document to provide assurance that operational procedures are consistent with contractual requirements.

Based on the content headings the operational procedures appear to be extensive in scope and categorise operational support procedures in terms of application area. This approach is commensurate with service industry documentation and lends itself well in providing the appropriate structure and level of detail required to support the live estate. The document is web-based allowing quick search and readily available guidance for support personnel. It is reported to be updated regularly in response to changes in support requirements and has formal approval sign of at senior level. It was evident from a brief review that the content of at least one application area was in the process of construction.

The procedures are designed to enable support personnel at any level to respond to any type of problem by providing clear guidance on actions required and appropriate escalation procedures. It supports the Problem Manager model indicating where necessary who is needed to support end-to-end resolution.

POL00394026

The procedures are also used to populate a Duty Manager's daily and weekly checklist. This provides assurance that scheduled operations are actioned in a correct and timely manner.

Extensive use is made of a pager alerting system via both BT pager and SMS messages to mobile telephones to alert both duty managers and operational support staff of issues that require resolution. This is managed automatically by the BTI system, which operates on dedicated servers at the Data Centres.

4.19 Supplier Management

ISD's involvement with suppliers is limited to dealing with them on a first line support basis. Contracts are let to third parties by ICL Pathway and ISD are only directly responsible for those elements under their direct control, namely NTL.

Regular monthly meetings take place between ICL Pathway, ISD and the suppliers where performance and issues are discussed. The suppliers provide monthly reports some days in advance of the meetings and these form the basis for discussion. Meetings are minuted and actions progressed and documented.

ISD did state that they are to introduce their own internal review cycle for NTL.

4.20 Audit Workstations

In February 2000 user testing of the Audit Workstations at both Wigan and Bootle identified that the required connections to the Audit Servers could not be achieved. PinICLs PC0037623 and PC0038167 were raised and while fixes have been developed and applied the opportunity to verify that the fixes had worked had not arisen.

Objective 3 of the audit was to prove that the Audit Workstations were now working as designed and could connect to their local Audit Workstation (eg. Wigan AW to Wigan AS) and to the remote one (eg.Wigan AW to Bootle AS). All four connections were proven and the PinICLs can now be closed.

5 Platform Configuration Audit Results

As part of the audit NT Systems belonging to the Horizon solution located in the Bootle and Wigan Data Centres were scrutinised for compliance to the latest build release produced by Pathway Development. The current release in the live estate being CI4S10.

The platform configuration audit consisted of two parts. Firstly, each cabinet containing NT systems was checked and the servers observed were recorded. The purpose here was to cross check the findings against RS/DES/054, the definitive statement of what should exist in the Data Centre. Secondly, "SDUSYSTEST", an automated tool was installed and executed on

POL00394026

a subset of the servers at each data centre. The subset of servers was determined by the NT Domains to which the servers belong. “SDUSYSTEST” generated a set of comma separated variable (csv) files. These files were collected from the Primary Domain Controller for each NT domain audited. In all cases the csv files and “SDUSYSTEST” were removed from the data centre servers after they had been captured onto a CD-ROM.

The captured audit files were analysed later at BRA01 using an Access database populated with the CI4S10 baseline configuration.

The results of the Cabinet Check can be found at Annex B to this report.

The results of the work using the automated tool can be found at Annex C to this report.

The detailed observations and recommendations of this element of the audit can be found at Annex D.

It is recommended that ISD draw up a Corrective Action Plan to address the observations made at Annex D and put into place those actions that will eliminate the weaknesses and n0n-compliances identified.

POL00394026

6 Annex A – Audit Terms of Reference

ICL PATHWAY	:	Internal Audit Terms of Reference
AUDIT TITLE	:	Data Centres & Belfast Operations
File Reference	:	AUD/3/4/32
Date	:	**5th October 2001**

Aim

The Pathway Data Centres at Wigan and Bootle and the Operations Centre at Belfast provide processing and support facilities for the Horizon network and other applications operated as part of the ICL Pathway project.

This audit will look at the ISD operations which are involved operating and supporting Pathway, including security matters, both at the Pathway Data Centres and Belfast.

The audit is part of the planned programme of internal audits for 2001 and was also identified as a pressing requirement in the audit of BS7799 Compliance, completed earlier this year.

The quality requirements expressed in ISO9001 : 2000 will be used as a basis for the work as will the requirements of BS7799:2000.

Objectives

1. To provide assurance to Pathway management that the activities of Pathway Data Centre and Belfast Operations Centre operations, with particular regard to their management and security processes, are controlled and in accordance with agreed arrangements, including :
   - Physical and logical access controls;
   - Management of backup procedures and media;
   - Contingency planning and disaster recovery;
   - User administration and token authentication (Belfast);
   - KMS procedures and controls (Data Centres);
   - Measurement of service quality and other operational performance indicators;
   - Analysis of problems, their root causes and means of containing/preventing them;
   - Maintenance of Data Centre procedures.

ISD staff will be given the opportunity to raise any problems or issues with regard to the management of systems in the Data Centres.

2. To provide assurance that the operational state of the Pathway Data Centre systems do not deviate from defined secure build specifications and that the correct security configuration of servers, workstations and domain controllers is maintained.

This Objective will be accomplished using an automated compliance “toolkit”, developed “in-house” by SDU System Test, the output of which will provide an indication of the current level of compliance with Build Scripts held in PVCS.

3. To provide assurance that the Audit Workstations at both Wigan and Bootle are fully operational and capable of being used.

Dates

The audit will commence 29th October 2001 with completion and draft report production and circulation targeted by 16th November. A final report will be issued together with the draft Corrective Action Plan by 23rd November.

POL00394026

Audit Resources

The Data Centre element of this audit will be conducted by Jan Holmes, Pathway Audit Manager. Graham Hooper, Pathway Security Manager will conduct the Belfast Operations part. Mark Ascot (IDPU) will carry out the configuration audits in support of Objective 2.

Reporting

The report reference will be IA/REP/036. The CAP reference will be IA/CAP/036.

At the conclusion of the audit a draft report will be produced and discussed with the auditees. A final report will be produced and distributed to the Director and Senior Managers of all departments covered by the audit, as well as the Managing and Programme Directors of ICL Pathway.

Further distribution will be at the discretion of Programme Management.

Based on the report content, a series of Corrective and Preventive Actions will be agreed and documented in a Corrective Action Plan. This will be issued, and the agreed actions monitored on a regular basis.

TOR Distribution

ISD

Andrew Gibson	:	Operations Manager
Paul Sandison	:	Data Centre Site Manager
Steve Gardiner	:	Service Manager
Colin Johnson	:	Network **Operations** Manager
Warren Welsh	:	NT Technician

ICL Pathway

Stephen Muchow	:	Managing Director
Martin Riddell	:	Customer Service Director
Peter Burden	:	Operations Service Manager
Mike Stewart	:	Service Manager
Tony Wicks	:	Business Continuity Manager
Peter Jeram	:	Director, Quality and Risk
Graham Hooper	:	Security Manager
Mark Ascot	:	IPDU

POL00394026

7 Annex B – Configuration Audit Cabinet Check Results

Data Centre	Server Name	Missing Server Names	Compliant with RS/DES/054	Comments
Bootle	PBOPWYDCS01		No	PDC for PWYDCS domain
	PBOBVPN01		Yes	
	BBOBVPN02		Yes	
	PBOBOPSS01		Yes	
	BBOBOPSS02		Yes	
	PBOWSLAM01		Yes	
Bootle	PBOBOO01		Yes	
	MBOMAS01		No	CP2903 should have removed this server
	MBOMSD01		No	CP2913 should have removed this server
	MBOHDG134		Yes	
	BBOPHG017		Yes	
	WBOISM01		No	ISD Insight Manager Server
Bootle	MBOAGE01		Yes	
	MBOAGE02		Yes	
	MBOAGE03		Yes	
	MBOAGE04		Yes	
Bootle	MBOVPN06		Yes	
	MBOVPN11		Yes	
	MBOVPN05		Yes	
	MBOVPN09		Yes	
	MBOVPN03		Yes	
	MBOVPN07		Yes	
	MBOVPN01		Yes	
Bootle	MBOVPM01		Yes	
	MBOVEX01		Yes	
	MBOVPN08		Yes	
	MBOVPN04		Yes	
	MBOVPN10		Yes	
	MBOVPN02		Yes	
	MBOVPN12		Yes	
Bootle	PBORMT015		Yes	
Bootle	MBOCOR01		Yes	

POL00394026

Bootle	MBOCOR02		Yes	
Bootle	MBOCOR03		Yes	
Bootle	MBOCOR04		Yes	
Bootle	MBOARC01		Yes	
Bootle	MBOACF01		Yes	
Bootle	MBOSTG01		No	ISD Staging Server
Bootle	MBOSSC01		Yes	
Bootle	WBOVDW01		Yes	
Bootle	MOXRAP01		No	Temporary until Oxford SS can accommoda their site
	MOXRAP02		No	Ditto
Bootle	MBOWING01		Yes	
Bootle	MBOWING02		Yes	
Bootle	MBOWING03		Yes	
Bootle	MBOWING04		Yes	
Bootle	MBOFLG01		Yes	
Bootle	PBOPWYFTMS01		Yes	
	MBOOCMS01		No	Expected name to be MBOOCM01
	MBOLAP01		Yes	
Bootle	BBOPWYKMS01		Yes	
	BBOPWYKMS02		Yes	
	MBOKMS01		Yes	
Bootle	BSBSCLIENT005		No	TIVOLI SYSMAN Systems
	BSBSCLIENT004		No	
	BSBSCLIENT003		No	
	BSBSCLIENT002		No	
	BSBSCLIENT001		No	
	BSBMASTER001		No	
Bootle	BSYSMAST001		No	
	BSYSCLIN001		No	
	BSYSCLIN002		No	
	BSYSCLIN003		No	
Bootle	BSYSINV01		No	

POL00394026

	BSYSCLIENT004		No	
Bootle	BRAINBUILDER5		No	
	BRAINBUILDER6		No	
	BRAINBUILDER4		No	
Bootle	BSYSDEL01		No	
	BSYSMASTER002		No	
	BSYSCLIENT005		No	
Bootle		BBOPPWYDCS01	No	Server not found
		MBOAGE05	No	Server not found
		MBOAGE06	No	Server not found
		MBOAGE07	No	Server not found
		MBOAGE08	No	Server not found
		WBOACC01	No	Workstation not found
		MBOACS01	No	Server not found
Wigan	BWIPWYKMS01		Yes	
	BWIPWYFTMS01		Yes	
	MWILAP01		Yes	
	MWIKMS01		Yes	
Wigan	MWIVPM01		Yes	
	MWIVEX01		Yes	
Wigan	MWIVPN12		Yes	
	MWIVPN11		Yes	
	MWIVPN10		Yes	
	MWIVPN09		Yes	
	MWIVPN08		Yes	
Wigan	BWIPWYDCS01		Yes/No	Labelled incorrectly. Real name is BWIPWYD
	BWIWSLAM01		Yes	
	BWIPWYMAS01		No	CP2903 should have removed this server
	PWIWOPSS01		Yes	
	BWIWOPSS01		Yes	
	PWIWVPN01		Yes	
	BWIWVPN02		Yes	
Wigan	WWIMAS01		No	CP2903 should have removed this server

POL00394026

	WWIMSD01		No	CP2913 should have removed this server
	PWIBOO01		Yes	
Wigan	PWIDLR048		No	CSR+ should have been removed at BPS withdrawal
	BWIPHG048		Yes	
	MWIACS01		Yes	
	WWIAUD01		Yes	
	MWIHDG084		Yes	
Wigan	MWIAGE01		Yes	
Wigan	MWIAGE02		Yes	
Wigan	MWIAGE03		Yes	
Wigan	MWIAGE04		Yes	
Wigan	PWIPWYKMS01		Yes	
	MWIFLG01		Yes	
	MWIOCM01		Yes	
Wigan	MWIVPN01		Yes	
	MWIVPN02		Yes	
	MWIVPN03		Yes	
	MWIVPN04		Yes	
	MWIVPN05		Yes	
	MWIVPN06		Yes	
	MWIVPN07		Yes	
	WWIVDW01		Yes	
Wigan	PWIRMT050		Yes	
Wigan	MWICOR01		Yes	
Wigan	MWICOR02		Yes	
Wigan	MWICOR03		Yes	
Wigan	MWICOR04		Yes	
Wigan	MWIARC01		Yes	
Wigan	MWIACF01		Yes	
Wigan	MWISTG01		No	ISD Staging Server
Wigan	MWISSC01		Yes	
Wigan	WSYSMASTER002		No	TIVOLI SYSMAN Systems
	WLCFTMR01		No	

POL00394026

Wigan	WTEC001		No	
	WTEC003		No	
	BRAINBUILDER2		No	
Wigan	WSYSCLNT005		No	
	WSYSCLNT003		No	
	WSYSCLNT004		No	
	WSYSDEL01		No	
Wigan	WSYSMASTER01		No	
	WSYSCLNT001		No	
	WSYSCLNT002		No	
	WSYSINVDLT		No	
Wigan	WSBSCLIENT005		No	
	WSBSCLIENT004		No	
	WSBSCLIENT003		No	
	WSBSCLIENT002		No	
	WSBSCLIENT001		No	
	WSBSMASTER001		No	
Wigan		MWIAGE05	No	Server not found
		MWIAGE06	No	Server not found
		MWIAGE07	No	Server not found
		MWIAGE08	No	Server not found

POL00394026

8 Annex C - Domains & Servers Audited with "SDUSYSTEST"

Domain	Server Name	Data Captured	Comments
PWYDCS	PBOPWYDCS01	Yes	
	BBOPWYDCS01	No	BDC does not exist, it should do
	WBOOPS01	Yes	
	BWIPWYDCS02	Yes	
BBOOT	PBOBOO01	Yes	
BPOCL	PBORMT015	Yes	
	BBOPHG017	Yes	
BOPSS	PBOBOPSS01	Yes	
	BBOBOPSS02	Yes	
	MBOCOR01	Yes	
	MBOCOR02	Yes	
	MBOCOR03	Yes	
	MBOCOR04	Yes	
	MBOWING01	Yes	
	MBOWING02	Yes	
	MBOWING03	Yes	
	MBOWING04	Yes	
	MBOARC01	Yes	
	WBOAUD01	No	
	MBOACF01	Yes	
	MBOACC01	No	
	MBOACS01	Yes	
	MBOOCM01	No	
	MBOSSC01	Yes	
	MBOAGE01	Yes	
	MBOAGE02	Yes	
	MBOAGE03	Yes	
	MBOAGE04	Yes	
BVPN	PBOBVPN01	Yes	
	BBOVPN02	Yes	
	MBOVPN01	Yes	
	MBOVPN02	Yes	
	MBOVPN03	Yes	

POL00394026

	MBOVPN04	Yes	
	MBOVPN05	Yes	
	MBOVPN06	Yes	
	MBOVPN07	No	
	MBOVPN08	No	
	MBOVPN09	No	
	MBOVPN10	No	
	MBOVPN11	No	
	MBOVPN12	No	
	MBOVPM01	No	
	WBOVDW01	No	
PWYFTMS	PBOPWYFTMS01	Yes	
	MBOLAP01	Yes	
	MBOFLG01	Yes	
WBOOT	PWIBOO01	No	
WPOCL	PWIRMT050	Yes	
	PWIPHG048	Yes	
WOPSS	PWIWOPSS01	Yes	
	BWIWOPSS02	Yes	
	MWICOR01	Yes	
	MWICOR02	Yes	
	MWICOR03	Yes	
	MWICOR04	Yes	
	MWIAGE01	Yes	
	MWIAGE02	Yes	
	MWIAGE03	Yes	
	MWIAGE04	Yes	
	MWIARC01	Yes	
	WWIAUD01	No	
	MWIACF01	Yes	
	MWIACS01	Yes	
	MWIOCM01	No	
	WWISSC01	No	
WVPN	PWIWVPN01	No	

POL00394026

9 Annex D – Configuration Audit Observations & Recommendations

No.	Observation	Recommendation	Action Required from Unit	Priority
1	RS/DES/054 has PDC for PWYDCS domain located in Belfast. It is actually located in Bootle.	Update RS/DES/054 to reflect PDC is located in Bootle and also BDCs located in Belfast.	IPDU Secure Builds	Medium
2	Servers MBOMAS01 and MBOMSD01 should not exist as part of the Bootle data centre.	Physically remove servers from Bootle data centre. Make the server available for re-use.	CS Security & ISD	Medium
3	WBOISM01 and MBOSTG01 are not recorded in RS/DES/054.	Include these servers in a future update.	IPDU Secure Builds	Low
4	APS Remote Gateways for Oxfordshire Social Services have been temporarily relocated into Bootle data centre. Need to investigate network access for this APS client. They use ftp to access their gateways. Can they use ftp to access Correspondence, Agents and Host servers?	Networks TDA to confirm access arrangements for Oxfordshire SS.	CS Security & Network TDA	High
5	OCMS Server at Bootle is labelled as MBOOCMS01. RS/DES/054 states it should be MBOCM01. Deviations can result in a failure to populate local group memberships and apply file security on a platform.	Confirm computer name. Update RS/DES/054 if required. Determine why deviations from the agreed naming conventions are occurring if required. PIT Secure Builds need server names to adhere to the stated naming convention in RS/DES/054.	ISD IPDU Secure Builds CS Security	Medium
6	TIVOLI SYSMAN System names differ from those recorded in RS/DES/054. No naming convention appears to have been followed for these systems, the names in Bootle differ slightly from those in Wigan.	ISD/SMG to provide IPDU Secure Builds with a list of server names and the stated convention for generating new server names. Update RS/DES/054 to include actual TIVOLI SYSMAN names or remove altogether.	CS Security ISD/SMG IPDU Secure Builds	Medium
7	Server BBOPWYDCS01 not found.	Confirm this server does not exist with ISD and update RS/DES/054.	IPDU Secure Builds	Low
8	Servers MBOAGE05 – 08 not found.	Update RS/DES/054 to remove these servers.	IPDU Secure Builds	Low
9	Servers WBOACC01 and MBOACS01 not found.	Confirm these systems do or do not exist with ISD and update RS/DES/054 as required.	IPDU Secure Builds	Medium
10	Server BWIPWYDCS01 is labelled incorrectly. The computer name identifies it as BWIPWYDCS02.	ISD to re-label this server correctly. RS/DES/054 to be updated to show server as BWIPWYDCS02.	IPDU Secure Builds	Medium
11	Servers BWIPWYMAS01, WWIMAS01 and WWIMSD01 should have been removed by CP2903 and CP2913.	Physically remove servers from Wigan data centre. Make the server available for re-use.	CS Security & ISD	Medium
12	Server PWIDLR048 should have been removed as part of BPS/DSS withdrawal.	Physically remove server from Wigan data centre. Make the server available for re-use.	CS Security & ISD	Medium

POL00394026

13	WWIISM01 and MWISTG01 are not recorded in RS/DES/054.	Include these servers in a future update.	IPDU Secure Builds	Low
14	The current installation log file generated by the PIT build scripts do not provide easy to find information regarding platform build, release, increment, fast track, work package identifiers.	PIT Builds to be enhanced to generate a separate log file which records a summary of the build history in terms of release, increment, fast track and work package identifiers.	CS Security & IPDU PTI	High
15	User account gstep01 does not appear to have been created from the secure template zzSYSMANDEV.	Need to confirm whether this user account complies with Pathway Security policy for user accounts. If it has not been created from the secure role then the account must be disabled and a new account generated from the said secure template.	CS Security & ISD	Medium
16	User account pspen01 created from a redundant secure role zzPWY FRM MAN.	Need to confirm whether this account is still active. If not then at the least it should be disabled if not deleted and removed from the system.	CS Security & ISD	Medium
17	SecurID is not installed on ISD Operational Support Workstations and therefore not used to authenticate with SecurID Token.	Confirm ISD have been given a dispensation to deviate from ACP/SFS.	CS Security	Medium
18	IIS has been installed a large number of platforms. It is only required on FTMS remote platforms	PIT to confirm platform builds do not install IIS. An action plan is required to remove IIS from the errant platforms.	CS Security & IPDU PIT ISD	Medium
19	Workstation WBOOPS01 is running SQL Server with Administrator account privileges instead of using a secure service user account.	CS Security determine remedial action required	CS Security	Medium
20	Platforms MBOACS01, WBOOPS01 and MWIACS01 are not running the TIVOLI Event Server Service (TecNT Adapter). This means these platforms are not forwarding NT events for auditing purposes.	PIT to confirm that the Auto Config Signing Server build does install and configure TecNT Adapter. ISD to configure TecNT Adapter on both AC Signing Servers and all ISD Platforms	CS Security & IPDU PIT ISD	High
21	Server MBOARC01 has D:\ shared with a share name of Richard. Correspondence Servers have a share for C:\ssc Server MBOLAP01 has a share of c:\smc These directories and shares are not documented in any design document and therefore are not secured, ie the directories will have Everyone: Change permissions.	Identify whether these are legitimate requirements. If they are, they should be protected with ACLs. If they are not required then they should be deleted.	CS Security & ISD	Medium
22	PBOPWYDCS01 PWYDCS PDC is populated with the following redundant Global Groups: PWY FRM MAN DSS FIT PWY FRM Analysts PWY FRM Users	Confirm action is required to remove these groups from PWYDCS domain.	CS Security & IPDU Secure Builds	Low

POL00394026

	RDMC Admin These groups should have been removed as part of BPS/DSS Withdrawal.			
23	Local group Rconsole Users exists on a number of platforms. Members of this local group are: PWYDCS\SSC Apps Man PWYDCS\SSC Apps Sup PWYDCS\Operational Man	Resolve use of remote access tools and legitimise configuration required.	CS Security	High
24	Administrator account is not being renamed as per the PIT build instructions. The IIS user account is present when it should not be.	These are both non compliance's with the Pathway Security Design. IIS user accounts should be removed or disabled at the very least. Administrator accounts is a long running problem.	CS Security	Medium
25	Audit Policy set on PBOBOPSS01 and BOBOPPS02 is not compliant to Security Design. Audit Privilege use is set on for Success and Fail.	IPDU Secure Build investigate determine whether this is right/wrong. And investigate PIT build for these two Domain Controllers.	IPDU Secure Build & PIT	Medium
26	Configuration of Event Logs is not compliant to the security design for: MBOARC01 MBOSSC01 MBOAGE01 MBOLAP01 MWIARC01	PIT investigate build configuration for these platforms. ISD to correct event log configuration.	CS Security PIT ISD	Medium
27	Configuration of user rights is not consistent for Correspondence Servers and Archive Servers. MBOCOR02, MBOCOR03, MBOCOR04 and MBOARC01 have Batch Logon Right which is not compliant with the security design.	PIT to confirm build is correct. ISD to correct user right configuration on these platforms.	CS Security PIT ISD	Medium
28	Examination of recorded logins shows that the highest account usage is by: PWYFTMS\Administrator PWYDCS\Administrator BOPSS\Administrator PWYDCS\pstee01 WOPSS\Administrator PWYDCS\lkian01	Use of administrator accounts instead of individual accounts means that auditing of individual actions is not possible. ISD to be reminded that individual accounts should be used.	CS Security	Medium

POL00394026

29	Account Policy is being by passed. Users are not being forced to change passwords at 30 days as per security design. This mainly applies to the operational management and SSC users, ie-privileged accounts.	CS Security and IPDU Secure Build review the policy.	CS Security & IPDU Secure Builds	Medium
30	Evidence exists that users who leave are not being removed from the system.	CS Security to review the policies regarding staff who leave.	CS Security	Low
31	User account tempftp suggests that an unauthorised user account has been created. As templates are not used in PWYFTMS domain this account will be full NT unsecured.	CS Security to investigate and review policy/processes. If necessary remedial action to be taken to remove this user.	CS Security	High
32	There are a number of global groups across the domains which are not populated with any members. This suggests that a number of the secure roles are not required. For example OCMS DBA does not have a user account.	Further analysis required and review with CS Security.	IPDU Secure Builds & CS Security	Medium
33	Two users have been configured that do not use the secure build login script: PWYDCS\mbeat01 PWYDCS\spark01	Both users are disabled until it has been determined why these user accounts are non compliant with the security design and policy.	CS Security & ISD	Medium
34	Duplicate templates exist for ACDB Admin and ACDB Users. This demonstrates that manual instructions passed from IPDU Secure Builds have not been processed by PIT and delivered to the Live estate. Mike Holms-Sharp strikes again.	Determine corrective action.	CS Security IPDU Secure Builds IPDU PIT	Low
35	The following accounts exist but are disabled: BOPSS\BMUIR01 PWYDCS\ABROW01 PWYDCS\AVAUG01 PWYDCS\RPATE01 PWYDCS\SKUMA01 PWYDCS\SSUR001 The creation of a user account in BOPSS is a fundamental breach of the Security Policy.	Determine corrective action.	CS Security ISD	Medium
36	The following user accounts are in more than one Secure Role: PWYDCS\DDILL02 ACDB Admin PWYDCS\DDILL02 OPERATIUONAL MAN PWYDCS\JSIMP01 SSC APPS MAN PWYDCS\JSIMP02 SSC APPS SUP	Determine corrective action.	CS security	Medium

POL00394026

	PWYDCS\NSTRE01 SSC APPS SUP PWYDCS\NSTRE01 ACDB Admin PWYDCS\PCARR01 SSC APPS MAN PWYDCS\PCARR01 SSC APPS SUP This is evidence that the processes used to manage user accounts are not being followed. Multiple roles for a single user account is a clear breach of the Security Design and policy.			
37	Server MBOACF01 has ISS installed and configured services set to auto. IIS should not be installed and the services should not be set to auto.	PIT to investigate platform build for this platform type.	CS Security & IPDU PIT	Medium
38	Servers MBOACF01, MBOACS01,MBOVPN03,MBOVPN04, MBOVPN05, MBOVPN06 have Compaq Web Agent Service configured and enabled. These services do not appear on the Wigan servers which says there is inconsistency between the servers. What is Compaq Web Agent and why is it on these platforms.	CS Security to investigate the use of this non standard service and inconsistency of VPN server and Auto Config server builds.	CS Security & IPDU PIT	High
39	Remote Console is installed and configured for use on 54 out of the 56 platforms audited.	CS Security to identify policy on remote admin. Currently this deviates from the intended security design and ACP.	CS Security	High
40	TIVOLI OBJECT Dispatcher (port 8002) is disabled on BWIPWYDCS02. It is running on all other platforms.	CS Security determine why this platform differs from the other. ISD to take corrective action.	CS Security	Low
41	SDUSYSTEST tool is needed as an online tool available to CS Security to access and audit live servers as and when required.	Update Security Auditors workstation to include SDUSYSTEST on its menu/toolset or develop special audit workstation for this task.	CS Security	High