ICL PATHWAY CHANGE PROPOSAL	**CP NO: 1987**
CP TITLE: Management & Support for System Penetration Testing	**DATE RAISED:** 17th May 1999
DATE BY WHICH CP TO BE IMPACTED: 24th May 1999 **RELEASE BY WHICH CP TO BE IMPLEMENTED:** LT2	**ORIGINATOR:** Barry Procter **SPONSOR:** Barry Procter
CP CLASSIFICATION: ~~FAST TRACK/~~URGENT~~/ROUTINE/BUDGET ONLY~~	**Line Manager Approval** Martyn Bennett (RECEIVED) Terry Austin (RECEIVED) NR2 ....
RELATED PinICL's: Not Applicable	

1. Description of Change Proposed:

The NR2 Delivery Forum approved the penetration testing exercise [overview below] on Monday 1st March 1999. (Penetration testing refers to both technical penetration testing and counter penetration testing.)

The attachment to this CP includes resource, rig, timing and budgetary information provided by Chris Wannell and Pete Dreweatt. The current Admiral assumption is that they may not be able to complete testing by 11th July – an impact statement is required from Systems.

Technical Penetration Testing:

Admiral Management Services Ltd [AMSL] to undertake independent technical penetration testing of ICL Pathway New Release 2 as described in their 'Penetration Testing High Level Test Plan' [HLTP]. ICL Pathway Security have provided advice for the development of this plan, which ensures that the proposed penetration testing will address the three major issues described at [2] below. The following framework is proposed:

That ICL Pathway provides a test rig during LT2 [see attachment]. Full technical penetration testing may then be applied in and end to end environment - fully exploiting all known, and potential, technical fraud and denial of service weaknesses;

At the end of testing, full configuration files are to be captured from the test system. No actual attack tests will be applied to the service in Live Trial, but test rig configuration files should be compared to ensure the live environment is an exact duplicate of the tested system.

Testing has been scoped around known technical vulnerabilities in a card-based payment system. The original BA-POCL 'Threat Schedules' have been reviewed to reflect the system as it has evolved. These threats, together with the application of contemporary technical attack tools, will form the framework to assure that no significant technical weaknesses exist in the Live system.

In addition to the provision of a test environment, ICL Pathway are responsible for:

□ The provision of access to the test environment for the testers;

□ A technical point of contact who will be available to assist the testers with such matters as installing test tools, creating and accessing test data (including user accounts), and interpreting IP network addresses;

□ A facility for testers, on a daily basis, to verbally inform the ICL Pathway IT Security Manager of any vulnerabilities found during testing;

□ The design and implementation of a counter (or solution), if any, to each vulnerability found during testing <u>if required</u>.

Counter Penetration Testing:

Counter Penetration Testing (CPT) is being undertaken to ensure that within reason, ICL Pathway has identified, prior to rollout, the counter processes where it may be exposed to an increased risk of attack from those seeking to perpetrate a fraud. The purpose is to identify where the documented (CS/PRO/023) counter procedures, when not adhered to, potentially open the system to fraud.

Testing is limited to NR2 functionality. The primary objectives are to determine for both Payment Card Distribution Facility (PCDF) and Benefit Encashment Service (BES) if fraud threats can be realised. This may be by deliberate or accidental actions of either Post Office counter staff or BA cardholders. Once threats have been identified then further testing will be undertaken to establish if they can be exploited.

Counter Penetration testing will need to be carried out during live trial and in a stable end to end test environment. Logically this could be the test rig set up for the purpose of conducting Technical Penetration testing. Transaction Management Service (TMS) records should also be available to enable tracking of the data elements of the various test scripts.

FRM staff will undertake the testing which is anticipated to take no more than ten days.

Summary of Requirements

□ An end to end environment incorporating multi post office and counter positions.
□ Population of the environment with, users, card batch details, customer records, payments records etc.
□ PUNS, payment cards, temporary tokens.
□ Support for the environment and technical backup.
□ Access to the TMS Journal for the system to allow the examination of events.

General:

Penetration testing is being carried out solely as an ICL Pathway activity and it is neither an Acceptance activity nor a contractual requirement. The results of the testing will be for ICL Pathway information only.

Following discussion with Chris Wannell, the preference is for this Penetration testing activity to take place in Bracknell.

2. Reason for Change:

Technical Testing:

The degree of confidence provided by existing technical security testing in Bracknell is constrained because:

□ Technical security testing is unit based - it is not applied in an ‘end to end’ environment. Each test failure is assessed for business impact, but a combination of test failures across domains may create a greater risk than the sum of the parts.

□ All testing is undertaken in a changing test rig environment. It is impossible to guarantee that every test rig configuration will be wholly duplicated in the live environment. Any errors or omissions may introduce security weaknesses not present in testing.

□ The multiplicity of SFS and ACP requirements is an indication of the system’s security complexity. The technical test team’s reports remark on ICL Pathway’s implementation against requirements but technical testing does not identify any unforeseen shortcomings in ICL Pathway’s security controls.

Technical penetration testing will supplement technical security testing. No duplication of effort will take place.

Counter Testing:

The nature of fraud is such that it constantly evolves and changes shape as those seeking to commit a fraud change targets and modify their methods to take advantage of perceived or identified weaknesses in systems. Counter testing is therefore solely for the purpose of providing an additional level of assurance to ICL Pathway concerning possible fraud risks.

3. Consequences if Not Approved:

ICL Pathway will be less able to assure the absence of potentially significant weaknesses in the Live system.

4. Pathway Impact Assessment Distribution:

*Requirements, *Design, *Development, *Implementation, *Test & Integration, *PIT, *Quality Management, *Architecture, *Customer Service, Y2000, Security, Risk & Fraud Management, Commercial & Finance

*MANDATORY IMPACT ASSESSMENT

5. External Impact Assessment Distribution:

Name:	**Organisation:**	**Contact No:**

FUJ00117496

N/A	N/A	N/A

6. Impact On Pathway WBS

WBS Code.	Man-days* (CP Analysis)	Man-days* (CP Implementation)	Capital	Schedule
TOTAL				

*

Where the CP is related to a PDA Change Request these estimates will form the basis of a charge to the customer. Please provide a brief explanation below of the requisite work as justification of the manday effort.

7. Impact On Products

Product Identifier	Description	Version to be Changed	Version to be Delivered	Schedule
N/A	N/A	N/A	N/A	N/A

8. Impactor Recommendation/Comments:

APPROVE/REJECT/NO COMMENT

IMPACTORS NAME:

EXTENSION NO:	**DATE:**

Change Administration Use Only

SCP No:	**CR No:**	**CCN No:**

FUJ00117496

```
------------------------------------------------------------------
                CHANGE PROPOSAL
------------------------------------------------------------------
ID: PWY_CP_1987                          Create Date: 17-MAY-1999 13:20:44
Status: WITHDRAWN                        Originator: Lisa Morcom (Change Management)

==================================================================================

Title
------
Management & Support for System Penetration Testing

==================================================================================

Related Items
-----------------
Info
1   PWY:CP_01987_1.A-CDATTACH;1 (Info)      Lisa Morcom (Change Management)
    (CP_01987_1.doc)
    CP 1987 ATTACHMENT 1

Related Child Change Documents
----------------------------------------


Related Parent Change Documents
-----------------------------------------


==================================================================================

Impact Notes
----------------

Commercial & Finance

CS:     Service Support
        Service Delivery
        Security & Risk
        Service Introduction
        Service Transformation
        Core Services

DEV:    ACE
        AASS
        Agent                                   No Impact
        APOP Admin WS
        Athene
        Audit
        AutoConfig & CtrSched
        Counter APS
        Counter EOL
        Cryptography
        Data Warehouse                          No Impact
        DELT
        Design Authority
        FTMS
        Host APOP
        Host APS
```

	Host DRS	
	Host LFS	New CP
	Host NPS	
	Host RDMC	
	Host TES	
	Host TPS	
	Infrastructure	
	MTAS	
	Maestro	
	Message Broadcast	
	Networks	
	OCMS	
	Ops Documentation	
	Proxy Delivery Service	
	Reference Data	
	Secure Builds	
	SMG	
	Tools & Emulators	
	VPN	
ITU:	RV	Impact
	Support	Impact
	SVI	
	TD	
PMSP:	Planning	
	Project Mgmt	
	Software CM	No Impact
Quality & Audit		No Impact

Fujitsu Reference Data Required
Post Office Reference Data Required
Post Office Dependency Exists

```
Archived Impact Notes
----------------------------
CM_HARDWARE_IMPACT=No Impact
T_AND_I_IMPACT=No Impact
TSC_AGENTS_DEV_IMPACT=No Impact
DWH_DS=No Impact
CS_OTT_IMPACT=Impact
IMPLEMENTATION_IMPACT=No Impact
RISK_IMPACT=Impact
QUALITY_IMPACT=No Impact
PTU_OTT_IMPACT=Impact
APDU_AGENTS=No Impact
APDU_DWH=No Impact
PTU_LST_IMPACT=Impact
TI_IMPACT=Impact
CS_REL_MGMT_IMPACT=Pending
=========================================================================

Action Messages
--------------------


Action Number:  4 Date May 20 1999 08:07:25 By: Hazel Salvat
```

IMPLEMENTATION DATACENTRES COMMENT (John Davies): No impact. 19/5/99

Action Number: 4 Date May 20 1999 08:22:48 By: Hazel Salvat
IMPLEMENTATION COUNTER HARDWARE COMMENT (Ian Openshaw): No impact. 19/5/99

Action Number: 4 Date May 20 1999 08:37:45 By: Hazel Salvat
IMPLEMENTATION COMMENT (Billy Herd): No impact. 19/5/99

Action Number: 4 Date May 20 1999 09:16:58 By: Martin Bailey
CM - SOFTWARE : Zero impact, HARDWARE : Zero impact.

Action Number: 4 Date May 20 1999 12:59:08 By: Lisa Morcom
COMMENT FROM JOHN WRIGHT:Barry,Note: re Temporary Tokens, the service & infrastructure are not yet established, thus DLR unable to produce TT's for any test purposes. Also am unsure whether counters can currently process TT's. I leave you to check.Regards, John.20.5.99

Action Number: 4 Date May 20 1999 14:08:17 By: Neil Forde
TECHNICAL INTEGRATION: No PIT impact. BRA01 Technical Testing: 2 man days planning, estimated 6 man days to build over 4 days, 4 man weeks over 3 weeks for NT and N/W support.

Action Number: 4 Date May 20 1999 15:34:38 By: Lisa Morcom
Architecture impact (Alan Ward)Review of test plans and tests 2 daysReview of Interim findings (as they occur) 4 daysReview of draft/final report 2 daysComment & recommendations on pen test vulnerabilities 3 days total 11 days20.5.99

Action Number: 4 Date May 21 1999 08:39:20 By: Lisa Morcom
SECURITY DEVELOPMENT IMPACT (Alan D'Alvarez):I have a number of concerns with this CP evolving around allocation of resources for this exercise.Currently, the majority of security test resource, staff and equipment, are 'tied up' on supporting LT2 activity until the 16th June. Alongside this, there is an urgent requirement for scoping NR2+ security testing to enable a fully supportable end to end Security Delivery Unit plan to be baselined within the Programme Office.There are additional issues with regard to the equipment allocation within the various Delivery Units to support technical testing. It is currently acknowledged that there may be a likely shortfall and activities are currently in hand to scope and address this issue. However, Penetration Testing will be a further requirement that needs to be part of this.Who has been assigned to manage the penetration testing exercise? Before further comment can be made, I require access to a resourced plan for this activity to understand how it may impact on the activities I require to be completed.20.5.99

Action Number: 4 Date May 21 1999 09:07:02 By: David Groom
QUALITY No impact

Action Number: 4 Date May 21 1999 09:25:31 By: Hazel Salvat
IMPLEMENTATION COMMENT (Dean Felix): No impact on training. 21/5/99

Action Number: 4 Date May 21 1999 17:24:52 By: Lisa Morcom
PR IMPACT (Anna Campopiano):No impact.21.5.99

Action Number: 4 Date May 24 1999 08:31:07 By: Hazel Salvat
IMPLEMENTATION MIGRATION TRANSITION COMMENT (Martin Taylor): No impact. 21/5/99

Action Number: 4 Date May 24 1999 16:05:40 By: Suzanne Gordon
BRA01TT: Two issues/impacts. The first is on the use of the Security/SysMan test rig for pen testing. The rig has already been earmarked for end to end volume rollout testing in this timeframe. The pen testers will probably not want to share a rig with other testers. Furthermore the recent reorganisation has identified issues with allocation of BRA01TT kit and personnel whose resolution will affect the implementation of this CP. Secondly, this pen testing has a strong business element to it. The current test rig has simple arrangements for simulating the business environment, with small numbers of payments being injected in order to test the security facilities. Some time would have to be set aside to introduce a representative business environment, say 20 mds. (CQ)

Action Number: 6 Date Jun 2 1999 09:19:25 By: Lisa Morcom
PCCB DECISION (MTG 130):DEFERRED - PCCB defer this CP as there are issues surrounding the allocation of test equipment.Action: B Proctor to discuss and agree testing strategy and timescaleswith C Quinn and report outcome to PCCB.2.6.99

Action Number: 6 Date Jun 2 1999 13:50:57 By: Hazel Salvat
IMPLEMENTATION SCHEDULING COMMENT (Steve Burgess): No impact. 2/6/99

Action Number: 6 Date Jun 3 1999 16:22:36 By: Lisa Morcom
COMMENT FROM BARRY PROCTOR/COLUM QUINN:Procter Barry:The requirement (my responsibility) has been accepted; It strikes me that the action must now be within the Development Directorate to nominate a Penetration Testing Manager who can resolve the kit allocation and any other anomolies.Colum.Quinn(a)icl.com:Barry, I was surprised to be included in this action. At the PCCB I raisedthe issue of allocation of kit because, due to the reorganisation, BRA01TTwinds up its activities 16Jun and its resources are being split between theDelivery Units and Business & Technical Conformance. It's not clear who isgoing to sort this out so my understanding was that the issue was beingreferred back to you as the CP sponsor/originator. I think the next step isfor you to identify and agree who is managing the pen testing activity.3.6.99

Action Number: 6 Date Jun 7 1999 14:03:14 By: Lisa Morcom
ACTION FROM BARRY PROCTOR:I have written to Colum Quinn seeking clarification.7.6.99

Action Number: 6 Date Jun 9 1999 07:28:14 By: Jan Holmes
Suspend, since the scope of this should be reviewed following BA withdrawal.

Action Number: 6 Date Jun 9 1999 08:51:43 By: Lisa Morcom
CUSTOMER SERVICE IMPACT (Janet Reynolds):(John Wright) Note: re Temporary Tokens, the service & infrastructure are not yetestablished, thus DLR unable to produce TT's for any test purposes. Also amunsure whether counters can currently process TT's. I leave you to check.(Mik Peach) The CP states that testing facilities, rig etc will be provided,and that "Following discussion with Chris Wannell, the preference is forthis Penetration testing activity to take place in Bracknell".On the assumption that this means the Solution Centre rather than the SSC,then there is no impact on the SSC.If the implication is that CS need to find the rig, and provide the requiredaccess facilities etc, then this would have a very significant impact on theSSC, and may not be possible at all.(Barry Procter) Mik, The intention is for TSC-equivalent to host andresource these tests.(Janet Reynolds) Zero Impact received from the following members of customerservice: Peter Robinson, Dave Fletcher, Dave Wilcox, Mike Stewart, MikeWoolgar, Richard Brunskil.9.6.99

Action Number: 6 Date Jul 13 1999 14:35:31 By: Graham King
Risk - events have now passed this CP by - the removal of BES and PCDF invalidates the original counter test objectives. This part of the CP needs review to ascertain whether the expenditure of resource on this activity is viable.

FUJ00117496

Action Number: 7 Date Aug 5 1999 15:57:14 By: Sue Rutherford
PCCB DECISION (Mtg NO.140):
WITHDRAWN: PCCB sanctioned the withdrawal of this CP. I.Honnor stated that due to the withdrawal of BES the scope of this CP had changed, however, the requirement to test on other aspects of the system remains.
05/08/99

----------- END OF CHANGE PROPOSAL PWY_CP_1987 ----------