**Document Title:** Fraud Risk Management Service Design

**Document Type:** Specification

**Abstract:** A description of the ICL Pathway Fraud Risk Management Service including: Service functionality, availability and Contracting Authorities requirements.

**Status:** First Issue.

**Distribution:**

**Pathway**

J. C. C. Dicks

M. H. Bennett

A. E. Oppenheim

S. M. Muchow

**Horizon**

G Lewis

P Jenner

**Author:** Graham King, Risk Manager

**Approval Authority:** M.H.Bennett, Director, Quality and Risk

**Signature/Date:**

**Quality Authority:** D. Groom, Quality Manager

**Signature/Date:**

**Programme Delivery Authority:** Gareth Lewis

**Signature/Date:**

# 0 DOCUMENT CONTROL

## 0.1

## DOCUMENT HISTORY

| Version | Date | Reason |
|---|---|---|
| 0.1 | 04/07/96 | Preliminary draft for discussion |
| 0.2 | 15/07/96 | Revised draft incorporating Customer comments |
| 0.3 | 24/07/96 | Revised draft incorporating Contracting Authorities Requirements and enhanced service description. |
| 0.4 | 31/07/96 | Final Draft |
| 0.5. | 22/08/96 | Final Revisions Incorporated for sign-off |
| 1.0 | 27/08/96 | Final Draft |
| 1.1 | 09/09/96 | Revisions incorporated for sign-off. |
| 1.2 | 20/09/96 | Final review by Contracting Authorities comments incorporated. |
| 1.3 | 10/10/96 | Internal review Comments incorporated |
| 1.4 | 17/10/96 | Draft for Customer Review |
| 2.0 | 14/11/96 | First Issue |
| 2.1 | 10/3/97 | Incorporates changes to reports for Release 1 CCN136 |
| 3.0 | 23/04/97 | CCN136 agreed |

## 0.2 ASSOCIATED DOCUMENTS

| Ref. | Version | Date | Title | Source |
|---|---|---|---|---|
| CR/FSP/004 | 2.0 | 27/09/96 | Service Architecture Design Document | ICL Pathway |
| Schedule B01 | | | Requirement 895 | Contracting Authorities |
| RS/SPE/0003 | | | Extended Verification Process Requirement | ICL Pathway |
| PAS/STR/0002 | | | ICL Pathway Release Contents Description | ICL Pathway |

## 0.3 ABBREVIATIONS

| | |
|---|---|
| BA | Benefits Agency |
| CMS | Card Management System |
| DSS | Department of Social Security |
| FRMS | Fraud Risk Management Service |
| MIS | Management Information System |
| PACE | Police and Criminal Evidence Act 1984 |
| PAS | Payment Authorisation System |
| PDA | Programme Delivery Authority |
| POCL | Post Office Counters Limited |
| PUN | Pick Up Notice |

## 0.4 Changes

### Expected Changes

A further requirement to report uniquely for the SSA.

Reports to be capable of being by BA or POCL region.

These changes will be subject to change control.

## 0.5 TABLE OF CONTENT

# 1 Introduction

The ICL Pathway Fraud Risk Management Service is intended to be an integral part of a joint programme between the Contracting Authorities and ICL Pathway working in partnership to minimise the potential and actual occurrence of fraud in the overall service. A separate joint author paper is required to define this partnership approach to Fraud Risk Management. The document will cover working processes and organisational structure for agreement by ICL Pathway and the Contracting Authorities. The Fraud Risk Management Service will be introduced through a phased release of FRMS functionality as defined in the ICL Pathway Release Contents Description (PAS/STR/0002).

# 2 Scope

The Fraud Risk Management Service (FRMS) will deal with the identification, monitoring and management of all fraud associated with / relevant to the ICL Pathway system and service via appropriate and effective controls (technical, managerial, procedural and personnel). Additionally ICL Pathway FRMS will provide information to support the investigation of individual fraudulent Benefit encashment transactions upon being informed that an investigation is in progress.

ICL Pathway's policy is to identify and minimise the risk of residual fraud relevant to the ICL Pathway system. It is recognised that the possibility of fraud incidents exists, both within and outside the boundaries of ICL Pathway's responsibility.

The strategy underlying ICL Pathway's approach is to identify high risk situations and opportunities for change to the overall service environment where necessary in order to:

- Minimise fraud exposure within the ICL Pathway solution.
- Provide an information service to the Contracting Authorities to aid in the investigation and in the minimisation of fraud. This will include the provision of information relating to individual fraudulent Benefit encashment transactions.

The objectives of the FRMS are to contribute to the reduction of fraud by providing:

- the Contracting Authorities with trend, pattern analysis which will aid the identification of fraud risk and appropriate mitigation actions;
- information that will aid in the investigation of actual and / or potential fraud incidents to the appropriate investigative body;
- certification relevant to operation of the system as required by PACE Act, 1984, Section 69;
- fraud awareness training to Post Office trainers, in conjunction with the Contracting Authorities;
- information for the investigation of system boundary related incidents and trends, e.g. counter staff related fraud, with the aim of developing improved procedures;
- analysis of incidents and trends within ICL Pathway's control, in order to develop enhancements to the system;
- facilities to change the service operation and controls where appropriate to reduce identified fraud risk;
- adequate resources to provide the FRMS.

# 3 Service Functionality

The FRMS will comprise three core elements:

- A management information system, to analyse trends, fraud losses and to profile data patterns. This is part of ICL Pathway's own MIS.
- A fraud monitoring system, to profile abnormal or irregular activity and identify potential or actual fraud incidents.
- Organisation, infrastructure and procedures to operate the service effectively and provide support for Contracting Authorities fraud control.

## 3.1 Database Service

The Fraud Risk Management Service will incorporate a database that will:

3.1.1.1 Allow transaction data identified as representing real or suspected fraud to be copied from the Data Warehouse to the FRMS Database. This will enable flags to be applied to monitor the progress of investigation.

3.1.1.2 Access and retrieve information relating to actual and suspected fraud, identified by the Contracting Authorities through a flagging system for agreement by ICL Pathway and the Contracting Authorities.

3.1.1.3 Allow flags to be altered that are attached to transactions which have been investigated for actual or suspected fraud. This will allocate the transaction and value to one of a number of loss categories, and will allow full accounting, fraud analysis and assist in the determination of liability.

3.1.1.4 Access and retrieve additional data required to support Fraud Risk Management from other ICL Pathway systems if such details will not routinely be available in the Data Warehouse.

3.1.1.5 Allow ad hoc trawls of the system for particular data types and reports to enable FRMS to monitor emerging trends and patterns of criminal activity.

3.1.1.6 Ensure that flagged data relating to actual and suspected fraud is retained within the FRM database for a period of time beyond that used for normal transactions to enable a full and detailed ICL Pathway fraud history to be compiled and used to determine future fraud prevention measures and as evidence.

3.1.1.7 Analyse the database using rules to identify potential fraud incidents; these rules require definition and agreement by ICL Pathway and the Contracting Authorities.

3.1.1.8 Allow the production of a range of standard and exception reports designed by ICL Pathway FRMS, in consultation with the Contracting Authorities.

3.1.1.9 Be sufficiently flexible to automatically produce reports according to parameters set, and allow ICL Pathway FRMS to amend these overnight. This only applies to the FRMS Database, those reports being produced from other parts of the system will require a longer notice period.

3.1.1.10 Be accessed by dedicated PC workstations.

3.1.1.11 Be fully auditable, password protected and able to produce activity logs for each operator including terminal ID, log on/off times and files/records accessed. This system will be automatic requiring no manual input by ICL Pathway FRMS management.

## 3.2 Support of Suspect Fraud Incident Investigation

ICL Pathway FRMS will use all reasonable endeavours to assist with the investigation of repudiated Benefit Encashment claims, including the timely provision of relevant data and documents from ICL Pathway's systems or services in a format suitable for analysis by the Contracting Authorities Investigative body.

## 3.3 Data Capture

3.3.1.1 In order to carry out effective Fraud Risk Management the system will be able to access and retrieve all information associated with fraudulent or suspect transactions. If all the information required in the data capture list is not available within the data warehouse, the FRM system will be able to retrieve it from other Pathway databases such as PAS and CMS.

3.3.1.2 The placing of fraud flags on particular transactions will instigate automatic retrieval of associated items of information, which may or may not be held within the data warehouse. ICL Pathway FRMS will only be able to place these flags once the repudiated transaction becomes known to the FRMS. Therefore a mechanism for passing this information from the Contracting Authorities to ICL Pathway FRMS is required. ICL Pathway FRMS will inform the Contracting Authorities of suspect events through an exception reporting process as ICL Pathway becomes aware of such occurrences.

3.3.1.3 Once a fraud has been confirmed and a final category flag relating to that event has been posted, the event will be linked to any appropriate previous reports. This will allow a full fraud and transaction history to be built up within the FRMS Database and hard copy reports to be produced.

3.3.1.4 The ICL Pathway FRMS Database will also allow information to be recalled by using any of the individual pieces of data as the search field.

3.3.1.5 The system will also have access control to indicate and prevent an ICL Pathway FRMS operator of the FRMS Database accessing data relating to an account deemed to be sensitive by the Contracting Authorities i.e. a National Sensitivity Indicator is set, unless authorised to do so.

## 3.4 System Availability

The system will have been fully tested and ICL Pathway FRMS operator training completed in the required timescales; these are for agreement by ICL Pathway and the Contracting Authorities.

The system will be available for on-line use by ICL Pathway FRMS staff from Monday to Friday 0900 - 1700, and at other times by prior arrangement although it will be possible to request and schedule reports outside these times subject to an escalation route. The escalation route requires definition and agreement by ICL Pathway and the Contracting Authorities. The method of report requests requires agreement by ICL Pathway and the Contracting Authorities and will be included in the joint authorship paper described in Section 1 of this document.

ICL Pathway FRMS will have on-line access to all ICL Pathway systems to retrieve data items in order to support urgent investigations and limit losses from major incidents.

Reports will be limited to those described in this document and Requirement 895.

## 3.5 Routine Monitoring and Reporting

ICL Pathway MIS will be capable of providing both standard and ad hoc reports. These reports will utilise the information captured by the MIS and will be able to report both at individual transaction and aggregated levels. It is expected that the key areas requiring analysis will change over time as the profile of attempted and actual fraudulent transactions changes and is identified. Key information fields used as categories for initial analysis of fraudulent transactions will include:

- Transaction volumes, values
- Location
- Transaction details, including type (foreign or home), time etc.
- Cardholder Details, e.g. Name and address
- Customer Type, e.g. Alternate Payee, Permanent Agent.
- User identification, e.g. Counter Clerk, Help Desk Operator, Authorised representative of DSS or POCL.

Standard reports will initially be those outlined in Requirement 895. ICL Pathway FRMS reporting will provide the flexibility for reports to change, within reasonable timescales, as the system evolves. The reports will be provided to a central Contracting Authorities location; further distribution and the related costs will be borne by the Contracting Authorities.

ICL Pathway will also make available additional reports which will initially include the following information:

### 3.5.1 Monthly

3.5.1.1 Total number and value of fraudulent Permanent and Casual agent transactions by region and as a percentage of all fraudulent agent transactions.

3.5.1.2 Total number and value of fraudulent transactions by loss category by region.

3.5.1.3 Total number and value of fraudulent transactions by region.

3.5.1.4 Monthly Trends Report

This report will be run for one or more regions and will contain the following four sections.

The user will input the month number and the region name(s).

**Impounded Cards**

This section lists the number of cards that have been impounded by reason code. The regional total is also displayed.

**Total Transactions**

This section displays the total number and value of transactions by benefit code by post office and the totals for the region. A second section of the report will show the total number and value of transactions by benefit type nationally.

**Foreign Transactions**

This section displays the total number and value of foreign transactions by customer type (payee role). The regional totals are also shown.

**Extended Verification Transactions**

The section of the report relating to the Extended Verification Process is described in the document, Extended Verification Process Requirement, RS/SPE/0003.

These reports will be presented as a month on month trend to assist in highlighting any significant changes.

### 3.5.2 Quarterly

3.5.2.1 Total number and value of all fraudulent transactions.

3.5.2.2 Average value of fraudulent transactions.

3.5.2.3 Total number and value of fraudulent transactions by benefit type.

3.5.2.4 Average value of fraudulent transactions by benefit type.

3.5.2.5 Total number and value of fraudulent transactions by customer type (Beneficiary, Appointee, Casual Agent, Permanent Agent).

3.5.2.6 Total number and value of fraud losses by type of loss category (not defined at this stage, but expected to include Card: lost, stolen, counterfeit).

3.5.2.7 Total number and value of foreign transactions by loss category.

3.5.2.8 List of PUNs reported not received but card collected.

3.5.2.9 At the end of each quarter a report incorporating the above in an aggregated format will be provided. The report will also detail any identified trends that fall outside of the above reports. These will be compared against previous reports in order to monitor long term fraud control.

### 3.5.3 Annually

3.5.3.1 At the end of each ICL Pathway financial year a full report incorporating the above quarterly reports in an aggregated format will be provided. ICL Pathway FRMS will also report on the identified trends occurring during the year. These will be compared against previous years in order to monitor long term fraud control.

All reports will be subject to agreement and joint change control. They will be forwarded to a central Contracting Authorities location; distribution, and the related costs will be borne by the Contracting Authorities.

All reports will be delivered in an electronic format.

## 3.6 Exception Monitoring and Reporting

The ICL Pathway Service Architecture will be capable of monitoring and reporting exception circumstances to the Contracting Authorities. Exact circumstances will be agreed by ICL Pathway and the Contracting Authorities. Information will be distributed internally by the Contracting Authorities.

Ad hoc analysis and reports will be provided, subject to agreement by the Contracting Authorities and ICL Pathway. They will include specific fraud analyses and encashment monitoring, in order to aid the Contracting Authorities fraud investigations. Results of the routine monitoring and reporting will be used as input to the format and content of the ad hoc reports.

These are:

3.6.1.1 Post Offices where the number of individual frauds are > than X.

3.6.1.2 Post Offices where levels of fraud loss is > X.

3.6.1.3 Post Offices where there is a higher than X incidence of fraudulent foreign and / or agent encashments. This will most likely be expressed as a percentage of total office transactions.

3.6.1.4 Post Offices where fraud losses > than X occur involving a particular type of Identification Document (where recorded) or extended verification procedures.

3.6.1.5 Manual Input Report - Weekly

This report lists Post Offices where the proportion of manual input transactions exceeded a limit on any one day during the week input. The report only displays the daily figures that exceed the limit and the percentage for the whole week. The user will input the week number.

The report is sorted by weekly average descending.

The report actually retrieves data for all days for the post offices. The user will use the BusinessObjects Alerter function to hide those days that are below the limit.

The use of Alerters is a basic user technique which is covered in the BusinessObjects User Training Course.

3.6.1.6 Post Offices where more than X fraudulent transactions are made by

Casual Agents.

3.6.1.7 Post Offices where more than X percentage of all transactions are fraudulent

3.6.1.8 Lost and Stolen Payment Card Report - Monthly

This report will be run monthly with the pre-determined rolling period set at six (6) months. It will report those Customers who have lost or had stolen two (2) or more Payment Cards in the rolling period.

It will contain Cardholder name, NINO, first line of address and Post Code. The report will be ordered by Post Code

3.6.1.9 Customers who have been issued with a second reminder PUN.

3.6.1.10 Customers who have infringed Change of Nominated Post Office rules (re CR/FSP/004, Service Architecture Design Document, Version 2.0, 27/09/96).

ICL Pathway will distribute one copy of these reports to a central Contracting Authorities location. Further replication and distribution will be at the expense of the Contracting Authorities.

All reports will be subject to agreement and joint change control and delivered in an electronic format.

## 3.7 Reporting Dependencies

ICL Pathway will only be able to provide a full FRM reporting and investigation support capability for those cases investigated by the Contracting Authorities if the Contracting Authorities notifies ICL Pathway of the instigation of an investigation into a suspected fraud.

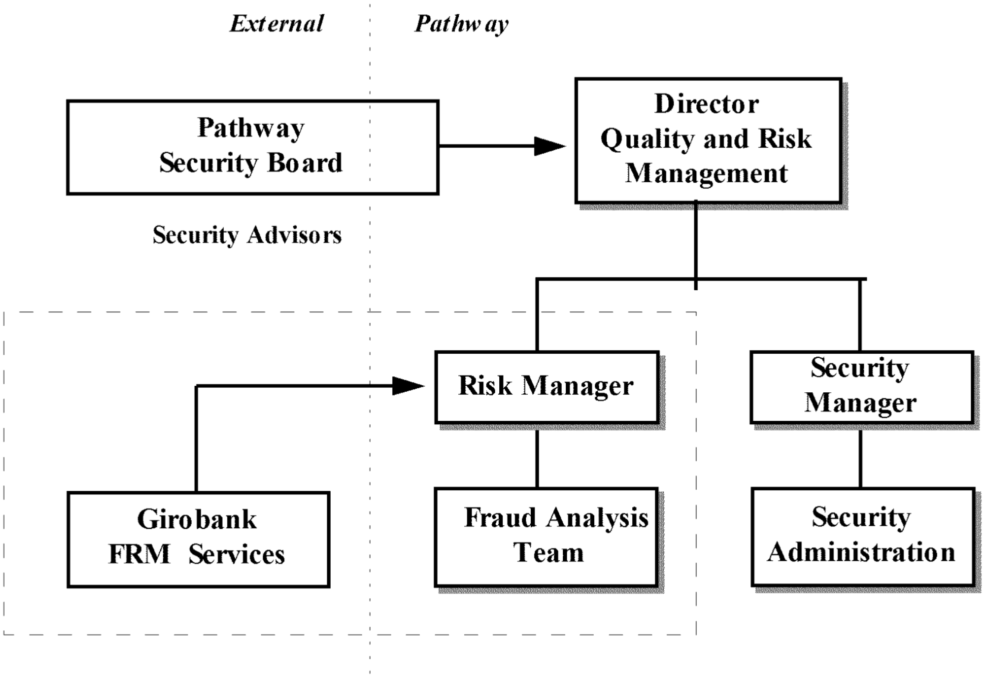
The reports used will change over time and will therefore be subject to agreement between the Contracting Authorities and ICL Pathway.

For the purpose of this document region is defined as being POCL Region unless otherwise stated.

# 4 Organisation, Infrastructure and Processes

## 4.1 ICL Pathway Fraud Risk Management Organisation

The ICL Pathway Fraud Risk Management service will have the following structure:



As illustrated specialist fraud and risk management services (notably those offered by Girobank) will be used to supplement Pathway's internal resources.

Use of external services enables:

- specialist skills to be invoked whenever needed,
- additional resources to be made available at short notice for special investigations,
- independent review of ICL Pathway's own procedures, and
- ICL Pathway to keep abreast of new methods for reducing risk.

## 4.2 Responsibilities of ICL Pathway FRMS

This section outlines the responsibilities of the key individuals. All members of ICL Pathway FRMS will liaise, at the appropriate level, with the designated Contracting Authorities team(s) in order to facilitate the cross fertilisation of ideas and communication of information.

ICL Pathway will report all identified actual or suspected internal fraud incidents that occur within ICL Pathway's domain to the Contracting

Authorities as they become known.

### 4.2.1 Director, Quality and Risk

The responsibilities of the Director, Quality and Risk Management, include:

- overall control of security throughout ICL Pathway,
- provision of adequate resources for security,
- being Chairman of the ICL Pathway Security Board (see section 3.2),
- approval authority for ICL Pathway's Security Policy,
- approval authority for ICL Pathway's Security Standards,
- overall control of fraud and risk management functions,
- establishing the security interface with the BA and POCL, and
- establishing the security interface with all subcontractors.

### 4.2.2 Risk Manager

ICL Pathway's Risk Manager's responsibilities include:

- identifying and categorising risks associated with fraud,
- analysis of trend incidents and fraud losses,
- fraud monitoring, to profile abnormal or irregular encashment patterns and identify potential fraud incidents,
- establishing internal controls to reduce the potential for fraud,
- in consultation with the Contracting Authorities establish external controls for the use of the ICL Pathway FRMS,
- operate in accordance with agreed Change Control Process,
- reducing the potential for fraud perpetrated through collusion,
- reviewing security policy and standards from a fraud perspective,
- providing the point of contact for reporting all fraud incidents,
- recording and investigating fraud incidents,
- management of the provision of information for the investigation of fraud incidents,
- managing the supporting FRM services, and
- liaison with external authorities in the event of fraud.

### 4.2.3 Fraud Analysis Team

The fraud analysis team carry out investigations relating to the cause of reconciliation failures and analysis of other fraud events as directed by the Risk Manager. The team's activities include:

- collecting and examining system evidence in support of investigations,

- reporting on the findings of all investigations,
- quantifying the amounts involved in fraud incidents,
- identifying persons implicated in fraud perpetration,
- recommending measures which could reduce fraud risks, and
- working with specialist external bodies developing new techniques.

# 5 Roles and Responsibilities

## 5.1 ICL Pathway FRMS

ICL Pathway's policy is to identify and minimise the risk of residual fraud relevant to the ICL Pathway system. It is recognised that the possibility of fraud incidents exists, both within and outside the boundaries of ICL Pathway's responsibility.

The FRMS will concentrate on the identification, monitoring and management of encashment fraud within the Benefit Payment Service and the POCL Strategic Infrastructure. ICL Pathway is responsible for the investigation of reconciliation failures, in order to identify where liability may exist and identify whether fraud was involved. Should fraud be suspected ICL Pathway will inform the Contracting Authorities and provide the relevant system information. ICL Pathway will use all reasonable endeavours to assist with the investigation of repudiated Benefit Encashment claims, including the timely provision of relevant data and documents from ICL Pathway's systems or services in a format suitable for analysis by the Contracting Authorities' Investigative body.

## 5.2 Contracting Authorities

The Contracting Authorities will be required to carry out investigation of Repudiation incidents and provide all reasonable support to assist ICL Pathway in the investigation of card issue failures. The Contracting Authorities will report events to ICL Pathway FRMS through the ICL Pathway Risk Manager. The Contracting Authorities will inform ICL Pathway, electronically, of any fraudulent or potentially fraudulent transaction they are investigating or have been informed of. This information will include flags relating to the type of fraud, suspected or actual.

The above information is required in order that ICL Pathway are able to provide the Contracting Authorities with the information to support the investigation of individual fraudulent Benefit encashment claims.

## 5.3 Procedures

The following procedures will be developed to ensure that communication channels between the Contracting Authorities designated security representatives and ICL Pathway Fraud Risk Management are developed with a partnership approach and information required to minimise fraud opportunities is easily utilised by all parties:-

a) Joint monthly meetings to discuss performance, fraud incidents and trends.

b) Quarterly Review processes to assess the effectiveness of :

- Report formats and content applicability.
- Mechanism for the investigation of fraudulent incidents.

- Other financial cards systems and any potential or impending changes in the industry.
- A process which will identify and evaluate potential changes to procedures and operations, for input to the joint change control process. This will ensure all information sources are used when determining fraud control measures.

c) An ongoing process of joint working and co-operation to ensure the best utilisation of joint assets.

d) A process for the exchange of information to support fraud investigations.

### 5.3.1 Actual and Suspected Fraud

On receipt of reports of suspected fraudulent incidents the officer to whom the report has been made, usually a BA local office staff member, will need to flag the transaction concerned to indicate a suspected fraud and, once the case has been investigated, to amend the flag to confirm the outcome of the investigation and, where appropriate, allocate the amount to one of a number of pre-determined loss categories.

It is envisaged that the flagging of fraud will require three separate actions by BA staff:

**A. Notification** - Why has the flag been raised - By whom - when.
(Suspected)

**B. Outcome** - What was proved to have happened.
(Actual)

**C. Allocation of Liability**

**A. Notification :**

As soon as an incident is reported the person to whom the report has been made must raise a flag through the procedure to be defined by the Contracting Authorities. This report is required to be passed to the ICL Pathway FRMS Database to identify the event under investigation and allow the retrieval and exchange of information to support the investigative process. Notification of actual and suspected fraud will be through an electronic interface.

The following are examples of key data requirements:

- Date
- Time
- Transaction Identifier
    - To Whom the report was made
- Reason e.g.:
    - Transaction repudiated
    - Extended Verification Procedure failure

These will need agreement based upon the experience gained during the live operation of the service.

**B. Outcome :**

Should it be established that fraud has not taken place the suspected fraud indicator will be removed and the transaction left as normal. The various categories require agreement with the Contracting Authorities.

When all action is complete a final closure category will replace the original notification flag and enable the system to record the established outcome. This will determine which category the amount fraudulently lost is posted to, which statistics will be affected and ultimately liability.

**C. Allocation of Liability:**

When finally allocated to a particular loss category the system will be able to produce reports totalling each category.

ICL Pathway require the Contracting Authorities to identify the party responsible for agreeing liability in order that a process may be defined and implemented. ICL Pathway's responsibility for agreeing fraud liability rests with the Risk Manager.

## 5.4 Staff Vetting

All ICL Pathway FRMS staff will be vetted in accordance with the ICL Pathway vetting procedures.

## 5.5 Training and Awareness

ICL Pathway FRMS will provide reasonable support to the Contracting Authorities training and awareness fraud control programmes.

## 5.6 Internal Controls

5.6.1.1 All PCs will be subject to access controls and located in a physically controlled environment with a full audit trail enabling ICL Pathway FRMS management to trace what information was accessed and by whom.

5.6.1.2 A separate Data Protection entry in the FRMS Database may also be required and the production of full operator activity sheets will allow management to investigate any alleged breaches of the Act. It will be possible to show who requested a report, when the request was made, when the information was made available and when it was finally accessed and, where appropriate, printed.