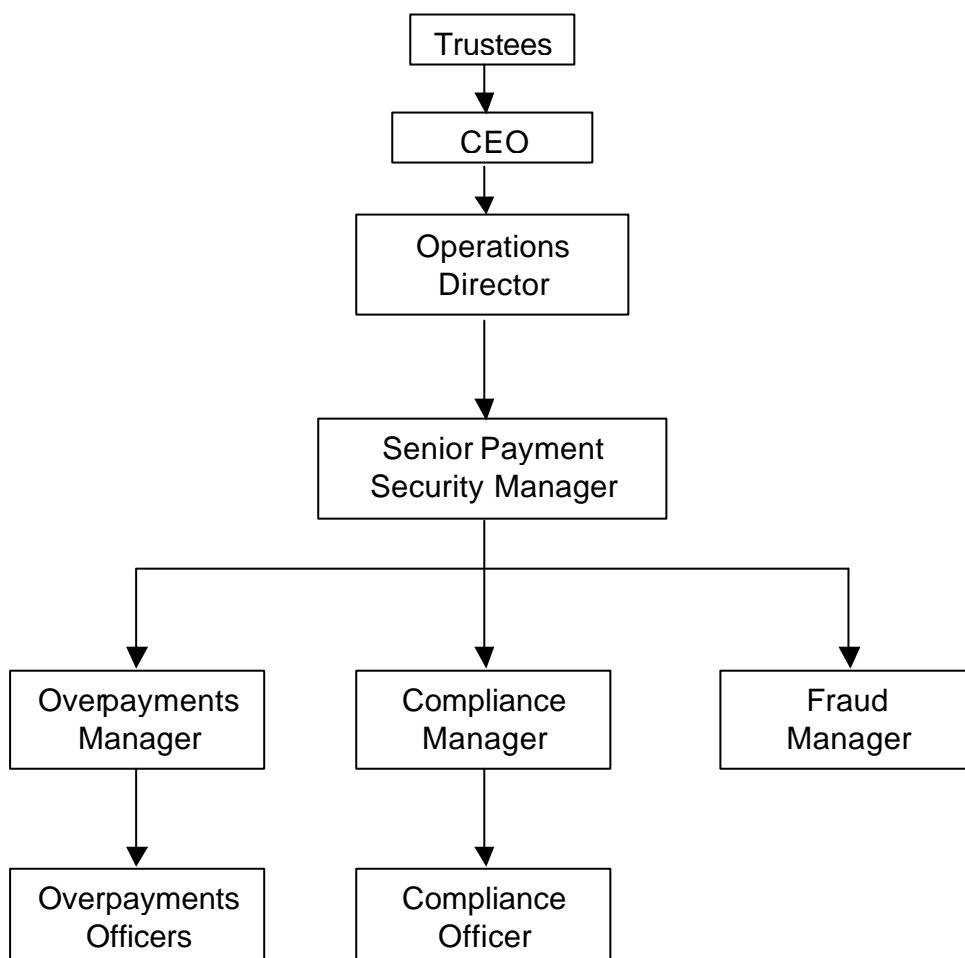


Appendix 3 – Payment Security Support and Assurance Structure

This document explains the overall structure relating to the Trustees and Chief Executive's delegation of various decisions and judgements to the Payment Security staff that determine and seek recovery of overpayments, and where necessary investigate allegations of non-compliance.

Payment Security Team Structure



Initial Recruitment

Payment Security staff are recruited through appropriate HR procedures and a full induction training is included before live casework is given to new staff. The three Payment Security Managers (Overpayments, Compliance & Fraud) train staff and monitor development, including casework, and there are three formal probation reports. These include performance assessment before an appointment is confirmed.

Formal Training & Working Practices

The Payment Security team work to clear internal guidelines set out in the Overpayment Principles Document and Fraud Procedural Manual. They also ensure that any decisions and investigative work are made in accordance with relevant legislation (i.e. Police & Criminal Evidence Act, Fraud Act 2006, Human Rights Act & Data Protection Act). In addition, they adhere to ILF Best Working Practices guide as a standard approach to good customer service.

The process of decision-making and delegation of duties is supported by process maps using “Triaster”, software that was purchased for this purpose. The process maps link to Payment Security guidance to offer clear guidance to staff on who is responsible for what. The Senior Payment Security Manager maintains this guide. The three Payment Security Managers reinforce use of the guidance in one-to-one and team meetings.

Policy and Guidance

Payment Security staff ensure they are kept abreast of new policies that may affect their decision-making process through the ILF Policy system “CETIS” (software which was purchased for this purpose) which is accessible via the ILF Intranet. Staff are advised by email or intranet message when policies are added or revised. They use the CETIS system to review and “accept” the policy. CETIS can be set up so that a brief knowledge questionnaire has to be answered before a policy can be accepted. The Senior Operations Manager – Client Service Delivery tracks acceptance of policies.

There are Control Checks on ‘live’ and ‘closed’ cases that relate to policies and ensure correct procedure. In the case of overpayments, as well as checking for financial accuracy, the Checker will look at whether procedure has been correctly applied. Individual errors are returned to the individual via their line manager for correction. Line managers use the control check information in “one-to-one” meetings with staff throughout the year, and may also discuss any error trends in team meetings. The Senior Payment Security Manager collates control check information and will also raise any trends with the relevant individual. Where general weaknesses in operational procedure are identified, additional guidance and targeted training sessions are provided.

Limits Of Authority

Limits of authority are set in procedural documents. (eg Overpayment write-off limits, who can authorise an interview taking place and under what conditions, when and how a case can be referred for prosecution).

The Overpayment Principles document and Fraud Procedural manual state the appropriate escalation route (eg Senior Payment Security Manager, Director, Trustees).

Some Control Checks require the Checker to examine compliance with delegated limits of authority. Where a Checker has had personal involvement in a case, the Control Check will be referred to the next level in the Line Management chain.

Management and assurance processes

Line Managers can obtain various case lists from the QUASAR/ICI system to check on work in progress. This provides opportunity for review of casework to date and checks on compliance with policies, processes and limits.

Where the Compliance and Fraud Team are involved in a case, they carry out a casework review prior to any visit and identify through a risk assessment any issues to be considered; agreement to visit is signed off by the highest-ranking Manager not involved in the visit.

The highest-ranking Manager not involved in the visit, in order to decide upon what further action is proportionate, reviews the visit. Likewise, reviews on Compliance case files are conducted on a regular basis.

Advice and Support

Referrals may be made internally to the Payment Security team if issues arise relating to payment assurance (e.g. the use and management of ILF money) arise. Payment Security staff may refer cases through the line management chain if they need advice on how to deal with a particular case. The final level is via the Operations Director to the User Personal Cases Committee, either where Trustees have reserved decisions to the Committee or where existing policy does not cover the particular case.