Comhairle Contae Dhún na nGall
Donegal County Council

INTERNAL AUDIT DEPARTMENT

FINAL REPORT

IA24/5 – INVOICE REDIRECTION FRAUD PREVENTION REVIEW

December, 2024

Table of Contents

1. Executive Summary

This audit was added to the 2024 Internal Audit Work Programme at the request of the Head of Finance following the admission in February 2024 by Westmeath County Council that it had been defrauded out of €515,000. The purpose of this audit was to examine the processes and procedures in place in the Accounts Payable Team (AP) of the Finance Section around how a new Supplier is setup on Agresso for payment and also where a supplier requests to change their bank details.

An initial draft copy of the audit report was issued to relevant staff on the 3rd March 2025. The responses and comments received have been included below, where relevant.

Internal Audit's findings and recommendations, where applicable, are detailed below.

1.1 Internal Controls – Policies and Procedures

The current Anti-Fraud and Corruption policy which was last updated in 2019 is not in line with current best practice in some respects such as the Local Government Code of Practice, (refer to section 7.2.1 for further detail).

It is recommended that the Anti-Fraud and Corruption policy is reviewed and updated accordingly at the earliest opportunity and subject to a regular review going forward.

Internal Audit also found that the main processes carried out by staff in AP are detailed in several user manuals/ guidance notes, however certain key steps involved in the change of bank details process are missing, such as the check of the [redacted]. The specific checks to be carried out on a change of bank details request are also contained in a single paragraph of narrative, (numbered 21 in the document). These could be set out in bullet point or a numbered format for greater clarity.

It is recommended that Management review the guidance notes around amending suppliers' bank details and ensure that all steps to be followed are included and set out in a clear format, for ease of reference.

1.2 Internal Controls - Segregation of Duties

Internal Audit found that there is insufficient segregation of duties around the process of changing a supplier's bank account details, despite the DCC Finance risk register stipulating this as a current management control mitigating the risk of Invoice Redirection.

One of the conditions of DCC's Crime Insurance policy is that IPB will not cover financial loss as a result of theft, fraud or dishonesty committed by a third party if there is no dual verification process in place to validate the authenticity of a change of bank details request.

It is recommended that an automated dual verification control is introduced, if possible, that requires 2 members of staff to authorise amendments to any supplier's bank details. In the event an automated control of this nature cannot be developed, then a second staff member should review the supporting documentation for the change of bank details and record this accordingly, to satisfy the insurance requirement.

Note: Internal Audit suggests that Management investigate whether [redacted] could be utilised to prevent the change of bank details from completing on Agresso until a second staff member of an appropriate level, has authorised the change

1.3 Internal Controls – Staff Training

Internal Audit found that while new staff receive adequate training in the new supplier setup and amendment process, the AP team have identified a specific fraud awareness course delivered by the Institute of Public Administration, (IPA) that would be beneficial.

It is recommended that all staff in AP are enrolled in the specific fraud awareness training provided by the IPA. Internal Audit also recommend that Management make contact with the Garda Crime Prevention Unit to ascertain if they have any additional guidance in respect of fraud prevention around payments to suppliers.

Finance Comments: DCC Finance Team had an Officer visit some time ago and delivered an awareness course. Unfortunately, this was before the appointment of the current staff in the section.

1.4 Amending Suppliers' Bank Details Process

Internal Audit found that the process followed by staff in AP when amending suppliers' bank details largely conforms to the guidance on preventing invoice re-direction fraud issued by the Banking and Payments Federation Ireland via the FraudSMART website.

It is recommended that management consider formalising the spot check on larger payments further discussed in section 7.3.2 to being a mandatory step in the process for all payments over a certain threshold, (this check involves staff reviewing the supplier's account on [redacted]).

2. Assurance Rating

This audit has been assigned an assurance rating of:

Level 2 – Adequate

See **Appendix 2** for Classification of Audit Assurance.

On the basis of the work carried out in this audit, Internal Audit found that there is a generally adequate system of risk management, control and governance throughout the operating procedures of the Accounts Payable section in respect of the new supplier setup process and the process to change a supplier's bank account details. The systems and processes currently in place are ensuring that objectives are achieved.

Some improvements have been suggested to enhance the effectiveness of the controls already in place.

3. Introduction & Scope

Invoice Redirection Fraud occurs when a business receives a fraudulent email claiming to be from an existing supplier, advising of new bank details for payment. They might not necessarily request a specific payment at the time of the notification, but the next legitimate payment will be made to the fraudsters account. This often results in significant financial loss which may not be identified until a reminder for payment is received from the legitimate supplier.

Invoice redirection fraud is on the rise globally and cost Irish businesses an estimated €8 million in 2022 alone according to FraudSMART, the fraud awareness initiative led by the Banking & Payments Federation Ireland (BPFI).

Local authorities in Ireland have also been the target of invoice redirection fraud in recent years. Westmeath County Council confirmed in February 2024 that it had been defrauded out of €515,000 which was paid to a third party. In 2014, there was also an attempt to defraud Meath County Council out of €4.3 million which was paid to a third party before being recovered from a bank account in Hong Kong with the assistance of the Garda money laundering unit.

In 2024, the Accounts Payable team in DCC setup [redacted] suppliers for payment and made [redacted] amendments to suppliers' details, (these amendments include change of contact name, change of bank details, email address etc).

The scope of this audit includes an examination of the following:

1. The processes and controls followed by Accounts Payable, (AP) staff in setting up new suppliers on Agresso to receive payment.
2. The processes and controls followed by AP staff in changing the bank details of a supplier once a request of this nature is received.

4. Objectives

The main objectives of this audit were:

- To determine whether the current procedures in place for verifying the bank account details when setting up new suppliers or changing the

bank account details of existing suppliers on the Agresso financial system, are adequate.

- Identify any weaknesses in the overall process.
- Make recommendations for improvement, if necessary.

5. Methodology

The audit will be approached as follows:

- Meetings and discussions to be held with relevant staff in the AP team in the Finance section.
- Completion of an audit questionnaire.
- Examination of relevant Agresso Financial System records.
- A review of any documented policies and procedures in AP in relation to supplier setup and changing supplier details on Agresso.
- Review of relevant DCC anti-fraud policies.
- Research best practice in invoice redirection fraud prevention

6 Relevant Legislation, Guidance and Circulars

- Local Government Code of Practice (2024)
- Governance Principles and Governance Framework for the Local Government Sector
- Overview of the Work of Local Government Audit Service 2022
- Local Government (Financial and Audit Procedures) Regulations 2014
- National Payment Strategy 2024

7 Findings

7.1 Staffing

The AP team in Donegal County Council (DCC) consists of [redacted] permanent members of staff who process weekly payment runs to all suppliers of goods and services to DCC and who have submitted an invoice. AP also process

other payments such as grant payments to businesses and individuals on an ongoing basis. The AP team consists of [redacted].

Internal Audit contacted the other Local Authorities that are designated as, 'Medium' size by the National Oversight and Audit Commission, (NOAC) to compare the number of staff and the grading structure of their Accounts Payable teams to that in DCC, (NOAC classify DCC as medium size). One of the Local Authorities contacted by Internal Audit has replied to date and the staffing structure of their AP team is as follows:

	Grade	Number of staff
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Internal Audit did not compare the duties performed by DCC's AP team to that of the other Local Authority however it is reasonable to assume they are similar in nature.

7.2 Internal controls

A robust system of internal controls which is regularly reviewed helps reduce the risk of fraud occurring. It is the role and responsibility of management to ensure effective controls are developed in order to reduce risk and promote best practice throughout an organisation.

Staff in specific units where payments are processed require a heightened awareness, specific training and a thorough understanding of invoice redirection and how it is perpetrated, to help prevent fraud. Internal audit has identified the following key internal controls which management have implemented, to minimise the risk of invoice redirection fraud occurring in DCC.

7.2.1 Policies and Procedures

It is the responsibility of DCC management to ensure that robust policies and procedures are in place to help safeguard council assets from Invoice Redirection fraud. Policies and procedure manuals provide a roadmap for day-to-day operations, ensure compliance with laws and regulations and can help reduce the risk of fraud or corruption occurring. These documents

should be regularly reviewed and updated to ensure they remain fit for purpose and comply with relevant legislation.

IA examined the following relevant policies and procedures as part of the audit;

- Supplier set up process notes (updated 2025)
- Corporate Risk Register (2024)
- Purchase to Pay end user (2013)
- Accounts Payable reference manual (2013)
- Anti-Fraud and Corruption policy (2019) (this includes the fraud contingency plan).

IA have found that some of these policies and procedures documents require updating.

The DCC Anti-Fraud and Corruption policy was last updated in 2019 and is not in compliance with current best practice in some respects. For example, The Local Government Code of Practice, Governance Assurance Requirements under principle 2, requires a fraud prevention policy to be reviewed and updated regularly and should be approved by both the Senior Management Team and the Audit Committee. Internal Audit found that no reference to the Audit Committee is included within the DCC fraud policy and can find no evidence that the original document was approved by the Audit Committee in 2019. Internal Audit also reviewed the anti-fraud and corruption policy of several other local authorities and found that they were recently reviewed and contained greater detail than DCC's policy in many respects.

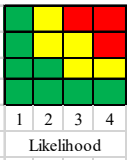
The Purchase to Pay user guide (2013) and the Accounts Payable reference manual (2013) are available for staff in AP to refer to as needed. Staff in AP have informed IA that these manuals do not cover supplier set up / amendments in the required detail and as a result have formulated their own supplier set up and supplier amendment notes with step-by-step instructions and associated screenshots. These supplier setup and amendment working notes are updated regularly with the most recent review conducted on 10th January 2025. Internal Audit found that while these notes largely cover the checks staff in AP conduct when processing a change of bank details, some steps are not clearly defined such as checking the [redacted]. The checks to be carried out on a change of bank details request are also contained in a single paragraph of narrative, (numbered 21 in the document).

IA examined the DCC Corporate Risk Register and found that a Crime Insurance policy was purchased from Irish Public Bodies Insurance company, (IPB) in 2021 as a control to mitigate against the impact of financial loss from fraud. Under DCC's Crime Insurance policy, [redacted]) the minimum standard to validate cover states that,

"There must be a dual verification process in place which validates the authenticity of any instructions by any payee (such as vendors or contractors) to amend their bank account details."

Internal Audit have found that there is no dual verification process currently in place when a supplier's bank details are amended upon request in DCC, (refer to section 7.3.2 below for further information on the process around amending supplier bank details).

The DCC Finance risk register was also reviewed, and invoice redirection is included as a specific risk as shown in the below extract;



Category of risk	Description of risk identified	Current management controls	Likelihood	Impact	New management controls	Responsible owner	Review dates
Financial / Legal	Fraud - e,g, staf theft, invoice/payment redirection, loss of property/assets	Internal control systems in place. Vetting of staff at recruitment stage. Segregations of duties. IT system protocols and approval limits/rights	2	3	Keep under review	Director of Finance	Ongoing

7.2.2 Segregation of Duties

Internal Audit is of the opinion that there is insufficient segregation of duties in relation to executing a supplier's request to change their bank details in DCC. IA was informed that only one member of staff actions the change of bank details process with no automated authorisation or recorded sign off required from either another member of staff or a line manager. Segregation of duties is listed as a current management control mitigating the risk of invoice redirection in the Finance Risk Register.

DCCs Anti-Fraud and Corruption policy also states that,

"No one person should have responsibility for recording and processing a complete transaction. Responsibilities should be divided to ensure that the key controls of custody, authorisation, recording, and execution are separated. Segregation of duties reduces the risk of intentional manipulation or error and increases the element of checking. Where segregation of duties is not feasible, this will be managed through closer supervision".

7.2.3 Staff Training

Staff training in fraud awareness is a key defence in recognising and preventing Invoice Re-direction fraud. Internal Audit interviewed the Staff Officer in Accounts Payable Team to ascertain the training procedures and resources available for staff in relation to setting up and amending suppliers in Agresso. These are as follows;

New staff

- When a new staff member joins AP, they are allocated their own user ID to access test Agresso, which is used for training, practice, and familiarisation purposes.

- There is 1 to 1 desk training provided by the [redacted]. The process for setting up / amending supplier details is explained in detail and the supplier set up and amendment notes are made available for reference at any time.

- When approval to work on the live Agresso system is granted, only straightforward supplier set up and amendments are assigned to the new staff member, which are then checked by the [redacted]. Once the new staff member is experienced and the line manager is satisfied with the standard of work, more complex requests are assigned to the [redacted] for completion, with appropriate checking completed by the [redacted].

All staff in AP

- On going training needs and development are identified in individual staff members' PDPs.

- Detailed user guides are available for all staff on the relevant [redacted].

- Staff attend quarterly Financial Management Systems team (FMS) meetings. The meetings are used to update staff on any current external threats and specific concerns of management and staff. It is also an opportunity to discuss new work practices such as the [redacted].

- Open, informal communication within the wider finance team on an ongoing basis can heighten employee's awareness of potential fraud. For example, all staff in AP were informed of the Westmeath County Council fraud, and the method used by the perpetrators in that case.

Staff in Accounts Payable Team made the following suggestions to Internal Audit to further increase awareness and reduce the risk of invoice redirection fraud occurring in DCC;

- Enrolment on a specific fraud awareness training course provided by the Institute of Public Administration should be considered for all staff in AP.

- Regular information sharing with the Garda crime prevention officer should be considered.

- Development of a specific training document for new staff joining AP that focuses on amending bank details.

7.2.4 Cybersecurity

In addition to adequate training and robust policies/ procedures, a strong cybersecurity framework is essential for the prevention and detection of fraud.

In DCC, the Information Systems department (IS) assists the various Directorates in maintaining cybersecurity around the various systems and programs used by staff. Some of the relevant controls in place include:

- Implementation of specific security software
- Completing system backups and recovery of data.
- Installing encryption software on relevant laptops.
- Restrictions are in place on Agresso which only allow designated staff in AP access to view and amend bank details.

- Access to most of the main systems used by staff is protected via a multi- factor authentication software ([redacted]).
- Guidance notes pertaining to invoice redirection, fraud awareness and cyber security are sent by IS to all staff via email and are visible on the staff hub. The last guidance note circulated in respect of invoice redirection was sent on the 29/10/2024. A guidance note in respect of fraud awareness (phishing) was also circulated to all staff in January 2025.

The [redacted] reported to Internal Audit that DCC is in the process of establishing a Cyber Security Unit within the organisation following the establishment of the Network and Information Systems 2, (NIS2) directive. This is due to be adopted into Irish law during 2025 and expands the scope of the original NIS directive, making cybersecurity obligations mandatory for a broader range of sectors, (including Local Authorities). The establishment of this unit should lead to cybersecurity protocols in DCC being strengthened and help protect against fraud.

A more detailed audit on cybersecurity in DCC is included on the 2025 Internal Audit workplan.

7.3 Set up process /amend bank details

Internal Audit interviewed the [redacted] in Accounts Payable Team who detailed the processes involved in setting up a new supplier and amending suppliers' bank details. The key steps are as follows:

7.3.1 New Supplier Set-up process

- A supplier set up request form is received by email to the [redacted], from [redacted].
- The form is checked by AP staff to ensure that the essential fields are completed i.e. [redacted]

- Agresso is then checked to confirm the supplier is not already set up [redacted] the form is a request for an amendment to the existing details and the process detailed further in 7.3.2 is followed.
- Using the [redacted] the next [redacted] is selected.
- [redacted]
- The [redacted] .
- [redacted]
- Providing that all the information received is correct, then the supplier is set up on Agresso for payment.

7.3.2 Amending Exisiting Suppliers' Bank Details

The process of amending existing suppliers' bank details is broadly similar to the new supplier setup process and is as follows:

- If a supplier needs to change their bank details, a request is submitted to Accounts Payable Team. AP can receive a request to amend bank details via the following [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]

- Any request from a supplier to change their bank details must be emailed. If AP staff receive a telephone call via the call centre, the supplier is advised to email the request.
- Once the request has been received and logged, the AP staff member checks the [redacted]
- [redacted]
- [redacted].
- There are [redacted] nominated Finance staff who receive an Agresso service report twice a week which notifies AP all changes of bank details.
- As soon as a payment is made to the supplier, [redacted]
- [redacted]

7.3.3 Test of Details – New Setups and Amendments

Internal Audit checked a sample of new supplier setups and supplier requests to amend bank details to ensure that the relevant documentation was received from the supplier and that the mandatory checks were completed by AP staff. The results were as follows:

Date	Supplier number	Request	Original email	Documents on file
08/02/2024	[redacted]	Change of Bank Details	Checked	[redacted]
27/03/2024	[redacted]	Change of Bank Details	Checked	[redacted]
26/08/2024	[redacted]	*	Checked	Completed Supplier set up form
26/09/2024	[redacted]	Change of Bank Details	Checked	[redacted]
06/12/2024	[redacted]	Supplier Set Up	Checked	[redacted]

IA found that four of the samples tested had all the correct documentation uploaded. [redacted]

* Supplier number [redacted] was a request forwarded from the Local Enterprise Office to check that the bank details they had received to make a payment, matched that which DCC held for the supplier. No change was made on Agresso by AP in this case.

7.3.4 FraudSMART Advice – Invoice Re-direction Fraud

FraudSMART is an online website created by the Banking and Payments Federation Ireland that offers advice to individuals and businesses on how to protect against various types of fraud, including Invoice Re-Direction. They

include specific advice for businesses to consider as a means of reducing the risk of invoice Re-Direction fraud including the following:

1. Make a phone call to a known contact within the firm that appears to be requesting fundamental changes in banking details.

2. Always verify any requests claiming to be from your creditors if they ask you to change their bank details for future invoices.

3. Always confirm change of bank account requests with the company making the change, being mindful not to use the contact details on the letter/email requesting the change.

4. Look out for different contact numbers and email addresses for the company as these may differ from those recorded on previous correspondence.

5. Consider reviewing change of account details already acted upon where payment is due at a future date and confirm the authenticity of the request.

6. Instruct staff with responsibility for paying invoices to be mindful of checking invoices for irregularities and voicing their concerns with the company requiring payment.

7. Consider setting up a system whereby when an invoice is paid an email is also sent to the recipient informing them that payment has been made and to which bank account. Be mindful of account security and consider including the beneficiary bank name and the last four digits of the account to ensure security.

8. Fraudsters may have found information regarding contracts and suppliers on an organisation's own websites. Consideration should be given as to whether it is necessary to publish information of this type in the public domain as it has been demonstrated that it can be used to facilitate fraud.

9. Consider setting up designated Single Points of Contact with companies to whom you make regular payments and for payments over a certain threshold, consider organising a meeting with the

company who are requesting payment, and satisfy yourself that payment will be sent to the correct bank account and recipient.

Internal Audit reviewed the processes within AP in relation to requests to amend supplier bank account details and compared it to the guidance above from FraudSMART and found that DCC conform to most of the key points already.

In respect of point 8 above, Internal Audit note that DCC have a statutory requirement to publish certain contract/ supplier information on the council's website, (this includes purchase orders greater than 20k and procurements greater than €20m).

In respect of point 9, AP staff advised Internal Audit that single points of contact are used where possible with the name recorded on Agresso, however this is not possible in every case due to the volume of suppliers DCC pay on an ongoing basis.

8 Conclusions & Recommendations

It is recommended that the findings in this report be considered, and that appropriate remedial action be taken where necessary.

8.2.1 Internal Controls – Policies and Procedures

Conclusion

The current Anti-Fraud and Corruption policy was last updated in 2019 and is not in line with current best practice in some respects such as the Local Government Code of Practice, (refer to section 7.2.1 for further detail).

Internal Audit also found that the main processes carried out by staff in AP are detailed in several user manuals/ guidance notes however certain key steps involved in the change of bank details process are missing, such as [redacted]. The

specific checks to be carried out on a change of bank details request are also contained in a single paragraph of narrative, (numbered 21 in the document). These could be set out in bullet point or a numbered format for greater clarity.

Recommendation

Internal audit recommends that the Anti-Fraud and Corruption policy is reviewed and updated accordingly at the earliest opportunity and subject to a regular review going forward.

It is also recommended that Management review the guidance notes around amending suppliers' bank details and ensure that all steps to be followed are included and are set out in a clear format for ease of reference.

8.2.2 Internal Controls - Segregation of Duties

Conclusion

Internal Audit found that there is insufficient segregation of duties around the process of changing a supplier's bank account details, despite the DCC Finance risk register stipulating this as a current management control mitigating the risk of Invoice Redirection.

One of the conditions of DCC's Crime Insurance policy is that IPB will not cover financial loss as a result of theft, fraud or dishonesty committed by a third party if there is no dual verification process in place to validate the authenticity of a change of bank details request.

Recommendation

It is recommended that an automated dual verification control is introduced, if possible, that requires 2 members of staff to authorise amendments to any supplier's bank details. In the event an automated control of this nature cannot be developed, then a second staff member should review the supporting documentation for the change of bank details and record this accordingly, to satisfy the insurance requirement.

Note: Internal Audit suggests that Management investigate whether [redacted] could be utilised to prevent the change of bank details from completing on Agresso until a second staff member of an appropriate level, has authorised the change

8.2.3 Internal Controls - Staff Training

Conclusion

Internal Audit found that while new staff receive adequate training in the new supplier setup and amendment process, the AP team have identified a specific fraud awareness course delivered by the Institute of Public Administration, (IPA) that would be beneficial.

Recommendation

Internal Audit recommends that all staff in AP are enrolled in the specific fraud awareness training provided by the IPA. Internal Audit also recommend that Management make contact with the Garda Crime Prevention Unit to ascertain if they have any additional guidance in respect of fraud prevention around payments to suppliers.

8.3.2 Internal Controls – Amending Supplier Bank Details Process

Conclusion

Internal Audit found that the process followed by staff in AP when amending suppliers' bank details largely conforms to the guidance on preventing invoice re-direction fraud issued by the Banking and Payments Federation Ireland via the FraudSMART website.

Recommendation

Internal Audit recommends that management consider formalising the spot check on larger payments further discussed in section 7.3.2 to being

a mandatory step in the process for all payments over a certain threshold.

9. Acknowledgement

I would like to acknowledge the assistance and co-operation of staff from the Finance Directorate and in particular those in Accounts Payable Team, in the course of this audit.

Gareth Park

Gareth Park,
INTERNAL AUDITOR

Appendix 1 – Circulation List

29/03/2025 Final Report sent to:

[redacted]

Copied to:

[redacted]

03/03/2025 Draft Report sent to:

[redacted]

Copied to:

[redacted]

Appendix 2 – Audit Classification

Level	Definition
1. Substantial	Evaluation Opinion: -There is a robust system of risk management, control and governance - The systems in place should ensure that objectives are fully achieved - The control processes tested are being applied consistently
2. Adequate	Evaluation Opinion: - There is a generally adequate system of risk management, control and governance - The systems in place should ensure that essential objectives are fully achieved - The control processes tested are, in general, being applied consistently - However, there are some weaknesses in control that are placing some objectives at risk. There is a risk that some objectives may not be fully achieved - Some improvements are required to enhance the adequacy and/or effectiveness of risk management, control and governance
3. Limited	Evaluation Opinion: - There is a weak system of risk management, control and governance - There is considerable risk that objectives will not be achieved - The control processes that exist are not being applied consistently - There are some significant weaknesses in control in a number of areas - Prompt action is required to improve the adequacy and effectiveness of risk management, control and governance
4. Unsatisfactory	Evaluation Opinion: - There is an inadequate system of risk management, control and governance - The system has failed or there is a real and substantial risk that the system will fail to meet its objectives - Systems/processes are open to significant error or abuse - Urgent action is required to improve the adequacy and effectiveness of risk management, control and governance
5. No Assurance	Evaluation Opinion: - Internal Audit has been unable to form an opinion on the system of risk management, control and governance - Internal Audit has been unable to access or has been prevented from accessing essential information required to form an opinion - Internal Audit has not received the cooperation of staff/management

Appendix 3 – IA24-05 Invoice Redirection Fraud Prevention Review - Summary Recommendations

	Material Issues Identified	***Actions Undertaken or to be undertaken***	***Timeline***	***Responsible Director & Service***
1	Internal audit recommends that the Anti-Fraud and Corruption policy is reviewed and updated accordingly at the earliest opportunity and subject to a regular review going forward. It is also recommended that Management review the guidance notes around amending suppliers' bank details and ensure that all steps to be followed are included and are set out in a clear format for ease of reference.	Anti-Fraud policy will be updated in line with LGMA template. Recommendations accepted and will be implemented	Q2 2025 for the Anti-Fraud Policy Q3 2025	Director of Finance & Director of Housing, Corporate & Cultural Services
2	It is recommended that an automated dual verification control is introduced, if possible, that requires 2 members of staff to authorise amendments to any supplier's bank details. In the event an automated control of this nature cannot be developed, then a second staff member should review the supporting documentation for the change of bank details and record this accordingly to satisfy the insurance requirement.	While a system-mandated dual verification is unavailable, there is a report that logs all changes. This report can form the basis of future controls. The wider Financial Accounts team is being strengthened and, as part of this process, enhanced segregation of duties will be introduced as regards supplier set-ups/amendments.	Q3 2025	Director of Finance
3	Internal Audit recommends that all staff in Accounts Payable Team are enrolled in the specific fraud awareness training provided by the IPA. Internal Audit also recommend that Management make contact with the Garda Crime Prevention Unit to ascertain if they have any additional guidance in respect of fraud prevention around payments to suppliers.	Finance Section has had continuing liaison with An Garda Síochána in specific cases and availed of a Garda briefing on fraud awareness in the past. Another formal engagement will be arranged. In addition, we will arrange fraud awareness training (with the IPA if it is	Q3 2025	Director of Finance

		deemed to be the best option available).		
4	Internal Audit recommends that management consider formalising the spot check on larger payments further discussed in section 7.3.2 to being a mandatory step in the process for all payments over a certain threshold.	Accepted and will be implemented as part of strengthening the Financial Accounts Team.	Q3 2025	Director of Finance