ITEM No …5……..

REPORT TO: **SCRUTINY COMMITTEE - 13 DECEMBER 2017**

REPORT ON: **FRAUD INCIDENT**

REPORT BY: **EXECUTIVE DIRECTOR OF CORPORATE SERVICES**

REPORT NO: **446-2017**

1 PURPOSE OF REPORT

1.1 To provide details on the serious fraud carried out by ex-employee Mark Conway and actions subsequently taken to ensure that the internal controls are strengthened and the risk of recurrence significantly mitigated.

2 RECOMMENDATIONS

2.1 It is recommended that Members of the Committee note:

- The background to, and the sophistication of, the Mark Conway case along with the immediate sequence of events and corresponding timelines that followed the initial discovery.
- The steps that have been taken to significantly mitigate the risk of recurrence within the Council.
- That the ex-employee, Mark Conway, pled guilty on 2 August 2017 to embezzling £1.065m from the Council and on 24 August 2017 at the High Court in Glasgow was sentenced to 5 years 4 months imprisonment.
- That, with the exception of £10,000 excess, the Council has recovered the £1.065m, in full, plus £47,141 towards the PwC fees of £55,804.
- The 2017/18 Internal Audit Plan contains two specific reviews, BACS and User Access Levels, to give assurances to Members and senior management around the related control environments. Going forward, as part of the 2018/19 Internal Audit Plan, a resource will be set aside to formally follow-up on all recommendations made by PwC to ensure that they have been implemented as intended.

3 FINANCIAL IMPLICATIONS

3.1 The overall value of the fraudulent transactions amounted to just over £1.065m.

3.2 With the exception of £10,000 excess, full recovery of this fraud has been achieved through a range of sources including Mark Conway himself, and the Council's Fidelity Insurance Policy. The Council has also recovered £47,141 towards the PwC fees.

4 BACKGROUND

4.1 As part of the Council's year end accounting work, the Corporate Finance Team holds the Council's ledger open for a period of time after 31 March to facilitate the recording of late invoices, for goods and services, that relate to the prior year. As a matter of routine, the Corporate Finance Team review invoices arriving after the year end to ensure that costs are captured in the correct accounting period. As part of this process on 20 May 2016 an invoice for £7,337 was queried.

Following initial enquiries, it became apparent that the normal process in place for tracing invoices within Civica Financials was not identifying sufficient corresponding purchase order and payment information.

The Corporate Finance Team made IT Services aware of the problem on 23 May 2016 via the IT Helpdesk. The call was assigned to Mark Conway, IT Officer, who subsequently advised Corporate Finance staff on the 25 May 2016, that he had been carrying out testing on the BACS system and used his own bank account details to test a payment, which had worked its way through into the live Civica Financials system and consequently made a payment into his personal bank account. Mark Conway immediately returned the payment of £7,337 to Dundee City Council.

Mark Conway had around 30 years' service with the Council and held the post of IT Officer. Mark Conway's role within the IT Service was providing support and assistance to mostly the Council's Civica Financials system and Bank Automated Clearing System (BACS) along with other financial systems.

Police Scotland was made aware of the suspicious transaction on the 30 May 2016.

Subsequent investigation and interrogation of financial systems by Council Officers uncovered 44 payments (including the first invoice), totalling £786,929, made to Mark Conway's personal bank account through the BACS system between March 2012 and May 2016. It was only possible to identify payments from March 2012 when the BACS system had been updated; there was no data available to review prior to that date.

At the same time as the investigation, a second bank account, suspected to be controlled by Mark Conway, was uncovered as a result of a City Development Transportation Service query relating to an April 2016 invoice for £17,846. This invoice was established to be suspicious as it had followed the same route as the other 44 payments noted above. The Council was able to establish that no other payments had been made to this account through the BACS system from 2012 onwards.

The total value of the 45 fraudulent payments to bank accounts known or suspected to be controlled by Mark Conway totalled £804,775. The payments ranged in scale from £5,898 and £27,557.

Police Scotland identified a further 12 transactions totalling £260,310 made between August 2009 and July 2012 and asked the Council to confirm that these payments had been made. Due to the information provided by Police Scotland around payment dates and values, further reports were requested from BACS and the Council was able to confirm that the payments had been made from a Council bank account into an account controlled by Mark Conway. From August 2009 to May 2016 the fraud totalled £1,065,085. Overall a total of 57 transactions over a 7 year period were identified using 2 separate bank accounts.

The fraud was carried out by Mark Conway using his expert knowledge of the Council's IT systems and his system access privileges. The fraud was carried out by inserting false invoices into the payment process. The invoices appeared to have come from the main systems but were not actually recorded in them. The invoices were payable to known suppliers.

Mark Conway was able to capture payments made against the fraudulent invoices and divert them to bank accounts within his control. Payments on genuine invoices submitted by suppliers were paid as normal.

There is no evidence available to the Council to suggest that Mark Conway acted in collusion with another party.

Mark Conway, pled guilty on 2 August 2017 to embezzling £1.065m from the Council and on 24 August 2017 at the High Court in Glasgow was sentenced to 5 years 4 months imprisonment.

4.2 **COUNCIL INVESTIGATION**

Once the first fraudulent payment was uncovered, Corporate Finance Staff notified senior management and it was agreed that Mark Conway should be suspended with immediate effect to allow for a full investigation to be carried out.

Mark Conway was suspended on Thursday 26 May 2016 and advised of the reasons behind his suspension. He was instructed to leave the premises immediately and not contact any members of staff or visit any Council buildings. All IT access was suspended immediately.

On Monday 30 May 2016, an investigation commenced under the Council's Disciplinary Procedure relating solely to the payment of £7,337 which had been processed to Mark Conway's personal account. Police Scotland was also notified of the incident. Mark Conway was invited to a formal disciplinary meeting on Thursday 9 June 2016 and at the conclusion of that meeting and prior to being issued with a notice of dismissal, Mark Conway tendered his resignation.

The Section 95 Officer of the Council at that time requested the support of PwC through the existing Internal Audit Co-source contract. Council Officers prepared a Statement of Work for PwC, which was to assist the Council to:

- Establish the extent of the anomalous payments and where they were sitting in the accountancy records;

- Establish where failings in the current control environment enabled this activity to continue without detection;

- Identify improvements to the control environment that would help prevent similar incidents in future; and

- Assess the resilience of the Council's systems to external threats.

The scope of the work was split into three distinct phases and agreement was to initially progress with the following:

- Understand the nature of the payments and how they were entered into the Council's systems;

- To confirm the location in the accounting records of the debit entries for the payments identified;

- To attempt to identify any currently undetected anomalous payments;

- Determine why the control environment surrounding the payments process did not detect these payments; and

- Suggest enhancements to the control environment that would prevent a recurrence of these payments.

The findings and recommendations from the work carried out is included at Appendix 1.

PwC notes in its report that the method used to extract the fraudulent payments was very sophisticated in comparison to other more commonly observed fraud cases.

The PwC report outlined the following six areas where internal controls could be improved:-

Ref.	Finding	Recommendation
1	***Restricted access for privileged system users*** The method used to process the fraudulent payments was the result of over-reliance on a single individual within IT who abused his privileged access rights. The user had access to systems right across the purchase to payable cycle and was able to use that access to execute the fraud.	Restricting system access rights, and, where possible, segregating responsibilities, limits the ability of any one user being able to bypass system enforced segregation of duties controls. An analysis should be undertaken across the Council's financially significant systems, to identify all system administrators and super-users. Where conflicting access rights exist, these access rights should either be segregated or, if segregation is not possible, then monitoring of that user's access should be implemented. The next step is to undertake a wider review of system access for all users across financially significant systems, focusing on identifying potential segregation of duties conflicts and defining the access users require for their job role and responsibilities.
2	***Interface reconciliations*** It is our view that effective interface reconciliation controls may have helped identify the fraudulent transactions earlier.	Controls should be implemented to verify the completeness and accuracy of the data being interfaced between sub-systems and the general ledger. Any differences identified should be investigated and resolved.
3	***Balance sheet reconciliations*** DCC did not conduct a balance sheet reconciliation from the Tranman sub-system to the general ledger. Such a reconciliation would have shown the fraudulent invoices 'routed' through this system. DCC did conduct a balance sheet reconciliation for the Construction sub-system but this was an ineffective control	It is recommended that DCC reconsider the balance sheet reconciliations that they are performing to determine if there are any missing reconciliations (such as the Tranman reconciliation) and whether the reconciliations that are currently taking place are effective.

Ref.	Finding	Recommendation
4	***Supplier statement reconciliations*** DCC did not conduct any supplier statement reconciliations on the supplier accounts that MC placed his false invoices into. While it is accepted that this may not be practicable for the construction sub-contractors, a monthly supplier statement reconciliation of the Scottish Fuels account should have revealed the fraudulent invoices that were 'routed' through the Tranman sub-system.	It is accepted that conducting supplier statement reconciliations is resource intensive, but we recommend that DCC consider whether they could conduct reconciliations on key supplier accounts, where it would be easiest to 'hide' fraudulent invoices.
5	***System limitations*** It is clear that the limitations of the current construction sub-system, DCS, have had a pervasive impact across the control environment, undermining the effective operation of segregation of duties, interface, and balance sheet reconciliation controls. Management have identified that the system is no longer fit for purpose and the process is underway to procure a new construction sub-system to replace the existing construction sub-system.	Until a new construction sub-system can be procured and implemented, management will need to consider the practicalities of developing a short term fix to address these issues.
6	***System and process documentation*** DCC do not have detailed system notes and mapping which articulate the flow of transactions and sets out how the interfaces work. This lack of documentation, while not a factor in enabling the fraud, was a contributing factor in the difficulty in tracking the accounting entries, as DCC could not demonstrate how the accounting systems actually worked. In order to gain an understanding of how the processes were working, PwC had to track entries through the systems, seeking to understand on a step by step basis what was happening at each stage of the process. This task, which was time consuming and labour intensive, would have been significantly streamlined had systems documentation been available. This lack of documentation places DCC at increased operational and financial risk should an unexpected event befall any of its IT systems in future.	DCC should document the processes and accounting pathways for each of its systems to ensure that they have a record of how these systems operate for future reference.

Recommendations 1 to 5 have been implemented in full. Recommendation 6 is nearing completion and is linked with the implementation of the new construction system which is planned to go live in August 2018.

4.3 RECOVERY OF FUNDS

The Council has insurance cover to protect itself against dishonesty of employees resulting in financial loss to the Authority. This type of insurance is called "Fidelity Guarantee" and local authorities are required to have such cover.

A summary of the cover is as follows:

- Insurer : Aviva
- Policy Limit : £2m any one claim in aggregate
- Employee Limit : £1m any one employee
- Policy excess : £10,000
- Provision within policy for external auditors fees in quantification of claim

Following discovery of the fraud and internal review of the Council's insurance cover, a formal claim was submitted to Aviva. The magnitude of the loss resulted in the following actions being taken by the Insurers all, of which are standard practice for large losses.

- Appointment of an independent Loss Adjuster
- Reservation of Insurers position
- Protracted exchange of information between the Council and the Loss Adjuster to satisfy the Insurer that the Council had met systems of checks and controls (which are conditions precedent to liability being admitted under the policy).

The manner in which the fraud was perpetrated was extremely complex.

Full recovery of the loss has been achieved excluding the policy excess of £10,000 through a range of methods including the pension of the convicted individual, an ex gratia payment through a third party and the fidelity insurance policy. In addition £47,141 towards the PwC fees of £55,804 was recovered under the fidelity insurance policy.

4.4 INTERNAL AUDIT

The Senior Manager – Internal Audit was one of the first members of staff to be made aware of the fraud and has been involved at key stages throughout the process, including the initial meeting of key officers, where Police Scotland was in attendance, and development of the initial Statement of Work for PwC.

The 2017/18 Internal Audit Plan, submitted to Scrutiny Committee on 19 April 2017, contains two specific internal audit reviews, BACS and User Access Levels, to give assurances to Members and senior management around the related control environments, which are associated to the fraud.

As part of the 2018/19 Internal Audit Plan, a resource will be set aside to formally follow-up on all recommendations made by PwC to ensure that they have been implemented as intended. A report on the findings from that review will be submitted to the Scrutiny Committee in line with standard reporting procedures. The Senior Manager - Internal Audit will now liaise with the Council's External Auditors, Audit Scotland, to complete and file the Council's Fraud Return for this case.

4.5 INCREASING RESILIENCE

The Council has strengthened its internal control environment recently with the establishment of an Integrity Group and a relaunch of the Whistleblowing policy and other related policies and procedure. These measures will assist in the detection and prevention of fraud risk.

A further piece of work was carried out by PWC which highlighted additional improvements surrounding the Construction IT system. These were recommended to enhance and strengthen the internal control environment. These have been implemented and focus on the following:-

- Journal, reconciliation and interface controls
- Process Improvements for journal entries for construction invoices
- Construction System and Civica Reconciliations
- Segregation of Duties within IT
- Super-User/Administrative Passwords

The Council has been approached by Police Scotland Safer Communities DETER who have a national remit for Prevention under Scotland's Serious Organised Crime (SOC) Strategy. Police Scotland have asked to work jointly with the Council to pull together a case study on the fraud that would be valuable in getting the resilience message across Scotland's wider public sector. This concept has been used previously and has prompted significant improvements to Public Sector resilience on a Scotland wide basis and links directly to the key objectives of DETER until the SOC Strategy.

5 **POLICY IMPLICATIONS**

This report has been screened for any policy implications in respect of Sustainability, Risk Management, Strategic Environmental Assessment, Anti-Poverty and Equality Impact Assessment.

6 **CONSULTATION**

The Chief Executive, Head of Democratic and Legal Services, Head of HR and Corporate Business Support and the Senior Manager - Internal Audit have been consulted on the content of this report.

7 **BACKGROUND PAPERS**

7.1 None.

Gregory Colgan
Executive Director of Corporate Services 29 November 2017

Dundee City Council Fraud Investigation – Report for Scrutiny Committee

04 December 2017

pwc

Contents

1 Background and introduction to this report

Subsequent to identification of what appeared to be a significant set of fraudulent payments to an employee, the Section 95 Officer of Dundee City Council (DCC), requested additional support from us through the existing draw down Internal Audit Co-source contract.

The support requested was to assist DCC to:

- Understand the nature of the payments and how they were entered into the Council's systems;
- To confirm the location in the accounting records of the debit entries for the payments identified;
- To attempt to identify any currently undetected anomalous payments;
- To determine why the current control environment surrounding the payments process did not detect these payments; and
- Suggest enhancements to the control environment that would prevent any potential recurrence of these payments.

At the conclusion of our work, we prepared a report setting out the full details of our scope, the results of the work performed and our conclusions. This report contained a high level of technical detail, much of which could be of value to a potential copycat fraudster. To address this point and to make the conclusions of our work more accessible, we were asked to prepare this report.

This report has been prepared for, and only for, DCC in accordance with the terms of our engagement and for no other purpose. We do not accept or assume any liability or duty of care for any other purpose or to any other person to whom this report is shown or into whose hands it may come save where expressly agreed by us in writing. To the extent that our report touches on points of law it should not be taken as expressing an opinion thereon.

We cannot guarantee that we have had sight of all relevant documentation or information that may be in existence, and therefore cannot comment on the completeness of the documentation or information made available to us. Any documentation or information brought to our attention subsequent to the date of this report may require us to adjust and qualify our report accordingly.

2 Initial discovery & quantification

DCC identified an anomalous invoice for £7,337 purportedly from a construction sub-contractor in April 2016 as part of their routine year end closure procedures. Investigation of this invoice determined that payment had not been made to the construction sub-contractor, but to the personal account of a DCC employee with 30 years' service, Mark Conway (MC), IT Officer, who had extensive access to a large number of DCC financial systems.

We understand that, when challenged, MC claimed that he had been running a test, that this was a unique incident and that there were no similar transactions. MC then returned the funds to DCC.

Subsequent investigation of payments to this bank account by DCC, through the BACs system identified 44 payments dating from March 2012 with a total quantum of £786,929 over the four year period. The BACs system was upgraded in March 2012 and DCC do not have sufficient records from the earlier version to be able to establish whether payments had been made to this account prior to the system change.

DCC had initially notified Police Scotland upon discovery of the initial unauthorised payment. The subsequent realisation of the quantum of funds involved resulted in DCC making an additional report to Police Scotland, and Police Scotland conducted an investigation into this matter.

Subsequent to the initial discovery a second bank account, suspected to be controlled by MC, was identified by DCC, as a result of City Development Transportation Service (CDTS) querying an invoice from a fuel supplier for £17,846. This invoice was established to be fraudulent and given that this invoice had followed the same 'route' as the £786,929 of invoices noted above, it was considered likely by DCC that this bank account was under MC's control, but this has not been confirmed. DCC were able to establish that no other payments had been made to this account through the BACs system post the BACs change in 2012.

The total quantum of these 45 known fraudulent payments to bank accounts known to be or suspected to be controlled by MC is £804,775. These ranged in scale between £5,898 and £27,557.

3 The mechanism used for these 45 payments

MC combined his knowledge of the DCC systems, and his system access privileges, to insert false invoices into the payment process. These invoices appeared to have been (but were not) recorded in either the in-house construction sub-system or Tranman, and were payable to known suppliers.

MC was able to intercept payments made against these fraudulent invoices and divert them to bank accounts within his control. Payments on genuine invoices submitted by these suppliers would not be intercepted, resulting in suppliers being paid as normal.

No evidence has emerged that MC acted in collusion with anyone else at DCC or with any external parties, including the suppliers for which he created false invoices. Collusion seems unlikely given the methods used but cannot be categorically ruled out.

4 Attempts to trace additional payments

DCC management were concerned that, given the sophistication of the fraud, there may be additional fraudulent payments that they were not aware of and so requested assistance from PwC, as their internal audit support partner.

With support from DCC we were able to use data analytics to run four separate tests to scan for additional fraudulent payments. The mechanism used to perpetrate the fraud had a number of distinct characteristics which are not present in most legitimate payments. We were able to scan the purchase records to identify all transactions with these distinctive characteristics.

These tests identified the fraudulent payments that were already known and a number of what, after subsequent investigation, proved to be false positives. We did not identify any other fraudulent payments beyond those already identified. However, given the natural limitations of data analytics, there remains a risk of further undetected accounts being used in the period subsequent to the introduction of the new BACs system in 2012

Due to system limitations, it was not possible to run any effective analytical tests on payments made through the pre 2012 BACs system.

5 Payments made through the pre-2012 BACs system identified by Police Scotland

Subsequent to the completion of the fieldwork and during the finalisation of the original report, Police Scotland identified 12 payments totalling £260,310 made between August 2009 and July 2012 which they asked DCC to confirm had been made by them. DCC were not made aware of the mechanisms Police Scotland used to identify these payments, but were able to confirm that they had been made from one of their bank accounts through requesting BACs reports for particular dates.

3 payments with a combined value of £64,615 appear to have been 'routed' through the Construction sub-system with the balance routed 'through' a now defunct Cleansing DSO sub-system. Due to system limitations it has not been feasible to determine the pathways of these payments and no further work has been performed upon them.

6 Accounting implications

We sought to trace the accounting pathways of all the known post 2012 fraudulent invoices.

The £501,406 of fraudulent payments 'routed' through the Construction sub-system can be traced to a suspense account in the general ledger balance sheet. With the exception of £7,337, which was reversed, it has not been possible to trace these payments leaving the suspense account. However, testing on the validity of the items within the suspense account at 31 March 2016 suggests that the fraudulent payments have been cleared out of the suspense account.

In the absence of being able to identify a pathway, it is impossible to be definitive about whether these items were routed to the P&L account or other balance sheet accounts. However, given the higher level of scrutiny over the balance sheet accounts as part of the year end process (which did not identify anything untoward), it is considered more likely that the fraudulent payments would be cleared to a P&L account rather than an another balance sheet account. Should that be the case, no further accounting actions are required in connection with these invoices.

A total of £303,368 of fraudulent payments over a four year period were 'routed' through the Tranman sub-system and these have been recorded within the P&L. No further accounting actions are required in connection with these invoices.

Given system limitations, it was not possible to determine the accounting pathways of the 'pre-2012' payments identified by Police Scotland.

7 Reasons for lack of detection of the post 2012 payments

As those transactions 'routed' through the Construction sub-system were not recorded in the Construction sub-system and cannot be identified on the general ledger out with the suspense account, it is unlikely that management would have been able to detect the fraudulent transactions from a cost review.

The high volume of invoices passing through the suspense account and the way that it operated would have made it virtually impossible for management to have detected these invoices from reviewing the suspense account on its own.

Limitations in the operation of the Construction sub-system prevented the imposition of a meaningful balance sheet reconciliation. Had such a reconciliation been possible, it may have revealed the fraudulent invoices as un-reconciled items that required investigation.

Given his knowledge of systems, MC may well have known of the system limitations when deciding on how to route the fraudulent invoices.

The expenses accounts that contained the fraudulent invoices 'routed' through the Tranman sub-system would have been subject to regular management review of costs. One of these fraudulent payments was detected by CDTS management reviewing the fuel costs recorded in the general ledger. It is not known why the remaining payments were undetected by management's cost review processes although the volatility of fuel prices may have helped mask the impact of these invoices.

8 Action Plan

Our review has identified a number of control weaknesses that enabled the fraudulent payments to go undetected. In the table below we have detailed our control findings and made recommendations to address the weaknesses. The method used to extract the fraudulent payments was very sophisticated in comparison to other more commonly observed fraud cases.

In our view, Dundee City Council is not alone among local authorities in Scotland in facing a challenging control environment, with limitations in the capability of IT systems and in staff and financial resource all having an impact. It is in this context that any recommendations for control improvements should be considered and any action taken to address the findings should be proportionate to the risk faced by not acting.

Ref.	Finding	Recommendation
8.1	***Restricted access for privileged system users*** The method used to process the fraudulent payments was the result of over-reliance on a single individual within IT who abused his privileged access rights. The user had access to systems right across the purchase to payable cycle and was able to use that access to execute the fraud.	Restricting system access rights, and, where possible, segregating responsibilities, limits the ability of any one user being able to bypass system enforced segregation of duties controls. An analysis should be undertaken across the Council's financially significant systems, to identify all system administrators and super-users. Where conflicting access rights exist, these access rights should either be segregated or, if segregation is not possible, then monitoring of that user's access should be implemented. The next step is to undertake a wider review of system access for all users across financially significant systems, focusing on identifying potential segregation of duties conflicts and defining the access users require for their job role and responsibilities.
8.2	***Interface reconciliations*** It is our view that effective interface reconciliation controls may have helped identify the fraudulent transactions earlier.	Controls should be implemented to verify the completeness and accuracy of the data being interfaced between sub-systems and the general ledger. Any differences identified should be investigated and resolved.

Ref.	Finding	Recommendation
8.3	***Balance sheet reconciliations*** DCC did not conduct a balance sheet reconciliation from the Tranman sub-system to the general ledger. Such a reconciliation would have shown the fraudulent invoices 'routed' through this system. DCC did conduct a balance sheet reconciliation for the Construction sub-system but this was an ineffective control	It is recommended that DCC reconsider the balance sheet reconciliations that they are performing to determine if there are any missing reconciliations (such as the Tranman reconciliation) and whether the reconciliations that are currently taking place are effective.
8.4	***Supplier statement reconciliations*** DCC did not conduct any supplier statement reconciliations on the supplier accounts that MC placed his false invoices into. While it is accepted that this may not be practicable for the construction sub-contractors, a monthly supplier statement reconciliation of the Scottish Fuels account should have revealed the fraudulent invoices that were 'routed' through the Tranman sub-system.	It is accepted that conducting supplier statement reconciliations is resource intensive, but we recommend that DCC consider whether they could conduct reconciliations on key supplier accounts, where it would be easiest to 'hide' fraudulent invoices.
8.5	***System limitations*** It is clear that the limitations of the current construction sub-system, , have had a pervasive impact across the control environment, undermining the effective operation of segregation of duties, interface, and balance sheet reconciliation controls. Management have identified that the system is no longer fit for purpose and the process is underway to procure a new construction sub-system to replace the existing construction sub-system.	Until a new construction sub-system can be procured and implemented, management will need to consider the practicalities of developing a short term fix to address these issues.

Ref.	Finding	Recommendation
8.6	***System and process documentation*** DCC do not have detailed system notes and mapping which articulate the flow of transactions and sets out how the interfaces work. This lack of documentation, while not a factor in enabling the fraud, was a contributing factor in the difficulty in tracking the accounting entries, as DCC could not demonstrate how the accounting systems actually worked. In order to gain an understanding of how the processes were working, PwC had to track entries through the systems, seeking to understand on a step by step basis what was happening at each stage of the process. This task, which was time consuming and labour intensive, would have been significantly streamlined had systems documentation been available. This lack of documentation places DCC at increased operational and financial risk should an unexpected event befall any of its IT systems in future.	DCC should document the processes and accounting pathways for each of its systems to ensure that they have a record of how these systems operate for future reference.