# *Aberdeen City Council*

## Compliance with the Public Records (Scotland) Act – Phase 2

Internal Audit Report 2014/2015 for Aberdeen City Council

**June 2015**

| | **Target Dates per agreed Internal Audit Charter** | **Actual Dates** | **Red/Amber/Green and commentary where applicable** |
|---|---|---|---|
| Terms or reference agreed 4 weeks prior to fieldwork | 08 July 2014 | 24 July 2014 | **Red** – Due to annual leave |
| Planned fieldwork start date | 30 March 2015 | 30 March 2015 | **Green** |
| Fieldwork completion date | 03 April 2015 | 03 April 2015 | **Green** |
| Draft report issued for Management comment | 17 April 2015 | 14 May 2015 | **Red** – Internal auditor on study leave |
| Management Comments received | 28 May 2015 | 28 May 2015 | **Green** |
| Report finalised | 04 June 2015 | 04 June 2015 | **Green** |
| Submitted to Audit, Risk and Scrutiny Committee | 25 June 2015 | 25 June 2015 | **Green** |

pwc

# Contents

# 1. Executive Summary

| Report classification | Total number of findings ← Section 3 → | | | | |
|---|---|---|---|---|---|
| | **Critical** | **High** | **Medium** | **Low** | **Advisory** |
| Medium Risk | | | | | |
| Control design | - | - | 4 | 1 | 1 |
| Operating effectiveness | - | - | - | - | - |
| Total | - | **-** | **4** | **1** | **1** |

## Summary of findings

1.01 The Public Records (Scotland) Act 2011 (the Act) requires Local Authorities to prepare and implement a Records Management Plan (RMP) that sets out proper arrangements for the management of records. We issued a report to the Audit, Risk and Scrutiny Committee, 'Compliance with the Public Records (Scotland) Act – Phase 1', on 20th November 2014 that set out several recommendations for management to implement to ensure Aberdeen City Council's (the Council) submitted RMP would be in compliance with the Keeper of the Records of Scotland's 14 element 'model plan'. The Council submitted its final RMP to the Keeper on 23 January 2015.

1.02 The initial scope of Phase Two of our review of the Council's compliance with the Act was to assess the design of the programme of controls testing to be implemented to help ensure the Council's on-going compliance and providing recommendations where improvements could be made. However, at the date scheduled for the fieldwork for our Phase Two review in March 2015, a programme of controls testing had not yet been completed or implemented, limiting our ability to perform the review in line with the scope agreed with management in July 2014.

1.03 Our approach for our Phase Two review therefore, was to assess the progress made to date on implementing the RMP, which is being achieved through an element of a wider improvement programme under the Council's the Information Management Strategy (IMS), and to highlight areas of weakness. We

interviewed key members of staff from the seven domains of information management outlines in the Council's IMS, and we reviewed key documents that evidence the progress made to date including the draft Information Management Strategy Risk Register. Since our Phase One review the Council has submitted its RMP to the Keeper. The Keeper assessed 12 of the 14 elements of the Council's RMP as 'Green', meaning "the Keeper agrees this element of an authority's plan". The two remaining elements were assessed as 'Amber', meaning "the Keeper agrees this element of an authority's plan as an improvement model. This means that he is convinced of the authority's commitment to closing a gap in provision. He will request that he is updated as work on this element progresses."

1.04 We have noted four medium risk and one low risk finding concerning the current progress in implementing the Council's RMP. The four medium risk findings are summarised as follows:

- Management stated that progress has been delayed in rolling out the Information and Records Lifecycle Management project (which will implement the Council's Business Classification Scheme and Retention Schedule), in part due to difficulties in recruiting suitable staff to the Information Management Adviser roles referred to in the RMP. Those responsible for the implementation of the RMP also highlighted the significant complexity involved in managing the wider IMS improvement programme across the Council. We found that the formal strategic plan setting the direction, actions and timescales for implementing the wider IMS improvement programme across the Council was still under development. In relation to the Information and Records Lifecycle Management project (which will implement the Council's Business Clarification Scheme and Retention Schedule, a series of pilot implementations are being considered and criteria for selecting participants is under development.

- 'Critical' and 'key' information management systems have not been consistently defined. Having a clear definition, consistently applied across the Council, is important to ensuring that information assets are properly managed in compliance with the RMP.

- Business continuity planning is not currently aligned to the requirements of the RMP submitted to the Keeper. We have identified areas for improvement in how Business Impact Analyses are prepared by Services and a lack of monitoring and reporting on compliance with review and test schedules for the Council's business continuity plans.

- Information Management related policies and procedures do not sufficiently detail how the Council ensures that access to information and data is appropriately removed for those employees who leave or move roles within the organisation. Physical controls have also not been implemented to restrict the ability of staff to save data outside of secure network drives, for example, preventing staff saving data to local hard drives or to portable devices such as memory sticks.

**Management comments**

This second phase of internal audit for 2014/2015 has provided management with the assurance that the Council's Information Management Strategy and improvement programme development underway remains aligned to providing the framework for governance of managing information across the Council. This form of internal review will be welcomed in the future to ensure the Council continue to develop and implement the required controls that support and inform the Council's use of information to deliver strategic objectives, and realise benefits for improving staff and customer experience.

# 2. Background and scope

## Background

2.01 Aberdeen City Council submitted their final Records Management Plan (RMP) to the Keeper of the Records of Scotland on 5th December 2014. The Keeper approved the RMP and provided an Assessment Report on 23 January 2015. The Keeper assessed 12 of the 14 elements of ACC's RMP as 'Green', meaning 'The Keeper agrees this element of [the] authority's plan'. It assessed the remaining two elements as 'Amber', meaning 'The Keeper agrees this element of [the] authority's plan as an improvement model. This means that he is convinced of the authority's commitment to closing a gap in provision. He will request that he is updated as work on this element progresses.' These two elements were element '4. Business Classification' and '5. Retention Schedule'.

2.02 The Information Management Strategy (IMS) has been developed to provide the framework for governance of information management across the Council. Successful implementation of the IMS is therefore key to ACC fulfilling the elements of its RMP in practice. The Information Management Team is developing an IMS Risk Register, which was in draft form at the time of our review.

2.03 The IMS Risk Register identifies risks to good information management and security and aligns these risks with the seven domains for information management that are identified in the strategy and in the RMP. These are:

- Business Continuity & Disaster Planning;
- Culture, Training & Communications;
- Information & Records Lifecycle Management;
- Information Preservation;
- Knowledge, Reuse & Performance;
- Risk & Governance; and
- Technical & Physical Systems Management.

2.04 The risk register aims will be the means by which the IMS improvement work as a whole will be driven and will be also be used to inform the assurance measures to be developed by each domain, which will form part of the improvement programme required by element '13. Assessment and review' of the RMP. The leads of

each domain will be responsible for developing and monitoring assurance measures for the risks associated with their domain, with the Senior Information Risk Officer (SIRO) holding overall accountability for the progress of the improvement programme.

2.05 The Information Management Team is preparing to roll-out the Information and Records Lifecycle Management improvement project (under the IMS improvement programme), initially to a pilot of three services, where they will test and refine the process for implementing the Business Classification Scheme and Records Retention and Disposal Schedule, these being the two elements identified by the Keeper for improvement. A budget for three Information Management Adviser posts has been approved, and two of these posts have now been recruited to. These roles will entail working with the pilot services to roll out the Business Classification Scheme and Records Retention Schedule by identifying the service's records and information systems, creating a file plan in line with Business Classification Schedule, and ultimately developing an Information Asset Register for the Council, in line with the broader aims of the IM strategy.

## Scope and limitations of scope

2.06 The detailed scope of this review is set out in Appendix 2 in the Terms of Reference. Our initial scope was to 'assess the design of the programme of controls testing, providing recommendations where improvements could be made'. However, at the agreed date of our fieldwork for Phase Two it was made clear by management that a programme of controls testing had not yet been completed or implemented, limiting our ability to complete the work in line with the scope agreed with management.

# 3. Detailed findings and recommendations

## 3.01 IMS implementation strategy and finalisation of IMS Risk Register – Control Design

**Finding**

IMS implementation strategy:

We have found that the formalisation of the strategy for the implementation of the IMS improvement programme as a whole across the Council is still on-going. The rationale for which services are to be selected for the Information and Records Lifecycle Management (IRLM) pilot implementation is also still being considered. The Records Manager is considering the first services to be included in the pilot as Children and Education, and either Housing or Planning, however no final decision had been made on those services that will be included in the pilot at the time of our review.

We recommend that the decision, on pilots, should be taken at senior level in the organisation with input of the leads of each service, based on a consistent and supported rationale for why each service has been selected. We would recommend the approach should include at least the following considerations:

- **Risk:** To consider the magnitude and likelihood of serious information security breaches in each service.
- **Cost and efficiency**: To consider the current cost of information management to services; for example, services with large volumes of paper records will incur high costs of storing their records, and services which could be using multiple IT systems could find cost and efficiency savings if information is being unnecessarily duplicated.

  There may be further efficiencies to be found where Services may be collecting and storing information that is already held by other Services within the Council and information sharing protocols are not in place.
- **User and staff experience:** To consider in which services better information management would have the greatest impact on user or staff experience of that service.

Information Management Strategy (IMS) Risk Register:

Management have not yet finalised and approved the IMS Risk Register. The IMS Risk Register is a key document in managing and monitoring information management risk across the organisation, and provides the basis for assurance measures and progress monitoring so that risks can continually be addressed, and improvement opportunities identified. It will also provide a point of reference for the Information Management Advisers when rolling out the IRLM project pilot to services to ensure all information risks for that service are identified and that there is plan for how these will be

addressed.

The final risk register should also incorporate a system of risk scores, based on the magnitude versus likelihood of each risk identified to enable management to prioritise addressing risks and considering whether other risks can be accepted rather than mitigated.

**Risks**

- There is a risk that the wider IMS improvement programme is rolled out to services without first identifying all of the information risks within that service, resulting in missing assurance measures to monitor all information risks. This will inhibit the wider IMS improvement programme from achieving best practice and efficiencies in information management within each service, and increase the risk of information security breaches occurring.
- There is a risk that the Council will miss the opportunity to prioritise services where the roll-out of the wider IMS improvement programme could have the most immediate impact in terms of mitigating the risk of information security breaches, creating cost and efficiency savings, and improving user or staff experience.
- There is a risk that the roll-out of the wider IMS improvement programme is delayed, which will delay benefits being achieved for services.

**Action plan**

| Finding rating | Agreed action | Responsible person / title |
|---|---|---|
| Medium | Management will finalise the formalisation of the plan for the wider IMS improvement programme, and agree the plan with the Corporate Management Team. The following actions will be prioritised:<br>• Finalise the Information Management Systems Risk Register;<br>• Formally select the services to be included in the IRLM project pilot implementation; and<br>• Identify the Information Asset Owners, Information Asset Administrators and Information and Information Management Liaison Officers within at least the three pilot services. | Records Manager<br>**Target date:**<br>30 September 2015 |

## 3.02 Identifying and maintaining business critical and key information assets – Control Design

**Finding**

We found that there is a lack of a clear, consistent definition of what constitutes 'critical' and 'key' applications and information.

While IT maintain a list of 'critical' and 'key' applications, it is not clear that consistent and appropriate criteria has been applied in identifying these applications. This is also not joined up with business continuity to ensure consistency in what is being identified as 'critical' rather than 'key' to each service.

There is also no formal monitoring and engagement with services to ensure that the list of applications is complete and up to date.

Identifying the business critical and key information management systems (including both electronic and hard copy systems) in each service is essential for the Information Management Team as they work with services to roll-out the Business Classification Scheme and in developing an Information Asset Register for each service. This is also an essential part of developing appropriate and relevant business continuity plans for each service.

**Risks**

- There is a risk that applications critical to Council Services' operations are not identified and classified as such, resulting in a lack of appropriate controls around information stored within these applications, including business continuity measures and controls relating to information security.
- There is a risk that applications that are not in fact 'critical' are inappropriately classified as 'critical', resulting in inefficient use of resources to develop business continuity plans for these applications, which are not necessary.
- There is a risk that without a complete list of key applications used across services, the Council will miss opportunities to identify potential cost and efficiency savings by eliminating unnecessary applications and unnecessary duplication of data across multiple applications.

| Action plan | | |
|---|---|---|
| **Finding rating** | **Agreed action** | **Responsible person / title** |
| Medium | Management will develop a clear definition of what constitutes 'critical' and 'key' information asset systems and ensure this definition is applied consistently across the whole Council.<br><br>Management will work with the Services to develop an Information Asset Register for the Council that documents:<br>• The location, status and criticality of key information management systems; and<br>• The owners of key information management systems. | Records Manager<br><br>**Target date:**<br><br>30 September 2015 |

## 3.03 Business continuity planning – Control Design

**Finding**

Business Continuity forms element 10 of the RMP, recognising that this is an integral part of good information management.

We performed a review of Business Continuity – Business Impact Analysis (BIA) Arrangements as part of the 2012/13 internal audit plan. This resulted in a high risk report. Amongst other issues, the report noted a lack of consistent engagement with business continuity across the organisation, resulting in some services having poorly documented or non-existent business continuity plans.

Since Phase One of our review of the Compliance with the Public Records (Scotland) Act, we found the Emergency Planning Team now have templates for BCP test exercises that it provides to services, and maintains a review and test schedule for each service with a BCP.

While element 10 of the RMP has been agreed and rated 'Green' by the Keeper's assessment report, we have found that in practice there are still actions to be taken to address the weaknesses previously identified by us in the Council's business continuity planning process, and to ensure that business continuity is fit for purpose across the organisation to align with good practice in information management.

In particular the following issues have been identified from the perspective of information management:

- Current arrangements rely on each service completing its own BIA template, which includes identifying business critical documents and systems.

  The completed BIA template then forms the business continuity plan for a service, where instead we would expect the Emergency Planning Unit to use the information provided in the template to perform a robust risk based analysis to formulate business continuity strategies and plans for that service.

- There does not appear to be a consistent definition or criteria applied in identifying 'business critical' information and applications (see finding 3.02 above).

- There is currently no formal system of monitoring and reporting on compliance with existing BCPs and compliance with the review and test schedule.

**Risks**

- There is a risk that information and systems that are critical to services continuing in the event of a disaster or emergency are not identified due to a lack of a clear definition of 'business critical' information and systems and a lack of robust review of the information provided in the BIA template. This could result in services being unable to access or recover critical information in such an event where plans are not sufficient to mitigate the risks.

- There is a risk that where there are business continuity plans in place these are not adequate or appropriate as these are not tested and updated on a periodic basis.

| Action plan | | |
|---|---|---|
| **Finding rating** | **Agreed action** | **Responsible person / title** |
| Medium | Management will re-evaluate the role of the Emergency Planning Unit (EPU) in business continuity planning and ensure that for each Service, the EPU performs a robust risk analysis of the Business Impact Analysis (BIA) to help Services develop appropriate business continuity plans.<br><br>Management will implement a formal process for reviewing and testing business continuity plans across the Council to ensure they continue to capture all critical business applications and systems and that those responsible for implementation of these plans are aware of their responsibilities in the event of a business continuity incident. | Emergency Planning Manager<br><br>**Target date:**<br><br>30 September 2015 |

## 3.04 Information management related policies and procedures

**Finding**

We have noted the following in relation to current information management related policies and procedures:

- We have reviewed five separate IT policies and procedure documents which are available for staff regarding IT security and data management. Much of the guidance, for example relating to portable devices, is repeated across all the documents reviewed.
- Some of these documents have not been recently updated, for example the ICT Good Practice Guidelines have not been reviewed since April 2013.
- During our inquiries the Information Security Officer identified the following control gaps:
  - There is not a robust procedure to ensure leavers or staff who change job roles have their access to all systems and network drives removed or appropriately amended; and
  - There are no controls to prevent staff from saving electronic data onto local drives rather than on the network, or from saving data onto portable devices that are not encrypted, which could include personal mobile devices such as mobile phones and tablets.

**Risks**

- There is a risk that staff will be unable to find the most up to date or relevant guidance to follow on IT security resulting in non-compliance with those policies.
- There is an increased risk of data breaches occurring when there are missing controls.

**Action plan**

| Finding rating | Agreed action | Responsible person / title |
|---|---|---|
| Medium | Management will review the current policies and procedure documents for IT and ensure that these are updated to reflect the new information management strategy. | Information Security Officer |
| | Management will review the processes and procedures in place for managing user access to information systems to ensure these are appropriate to mitigate the risks of unauthorised access to data. | **Target date:** |
| | Management will review controls over electronic data to identify actions that can be taken to restrict the ability of users to bypass controls over the storage of Council data on non-Council devices. | 30 September 2015 |

## 3.05 Data protection

**Finding**

From reviewing the Council's current Data Protection policy it was noted that it does not clearly cover internal information sharing within the Council. Such information sharing can sometimes be necessary or create efficiencies; however, it could equally be in breach of data protection laws similar to the sharing of information externally.

The Information Management Team are aware that some Services have information sharing protocols with each other; however, this is not always the case and could result in information being shared inappropriately within the Council, or result in missed opportunities where it would be appropriate and more efficient for services to share information.

The Council's current Data Protection policy is in the process of being updated, with the aim of the new policy being approved at Committee in May or June 2015. The existing policy had not been updated since April 2012, and we welcome the Council's pro-active steps to bring the policy into line with current good practice guidance and the aim to make a document that is more accessible for staff. In line with refreshing the policy and procedures, we understand that a new set of data protection training is also being designed.

It was noted in Phase One of our review that the Council does not currently keep a register of the information shared with external parties. We recommend that such a register is developed and regularly monitored.

**Risks**

- There is a risk that the Council fails to fully comply with data protection legislation, and is not aligned with good practice in this area, if the data protection policy is not regularly reviewed and updated.
- There is a risk that information is being shared internally in breach of the Council's data protection responsibilities, or that opportunities for efficiency in the sharing of data internally is being missed.

**Action plan**

| Finding rating | Agreed action | Responsible person / title |
|---|---|---|
| Low | Management will develop a Register of Information Sharing Protocols as a resource for staff to consult for clarity on the circumstances and types of information that can and cannot be shared internally. | Information Governance Officer |
| | Management will finalise updating the Council's Data Protection policy with consideration given to the possibility of streamlining the existing Data Protection procedures. Management will ensure the new policy is subject to regular, ongoing, review for compliance with current legislation and alignment with good practice. | **Target date:** 30 September 2015 |

## 3.06 Information management in supplier contracts – Advisory

**Finding**

As the Council implements its new information management strategy it should consider how this impacts on its relationship with suppliers and third parties who handle Council data. Suppliers who handle Council information should be expected to meet the same standards on information management as required by the RMP and IM Strategy and supporting policies.

It is recommended that procurement should review existing procurement policies and procedures to ensure these adequately refer to the IM Strategy or advise on appropriate reference to information management standards to be included in supplier contracts. A standard wording, to be included in all contracts, could be developed and included within the Corporate Procurement Policy.

The Council should also considering reviewing existing contracts with suppliers, and updating where required, to ensure there is adequate reference in these contracts on the supplier's responsibilities when handling or accessing Council data, particularly contracts within higher risk areas e.g. social care, education, and IT contracts where third parties may have access to personal data on employees and service users.

**Action plan**

| Finding rating | Recommendation | Responsible person / title |
|---|---|---|
| Advisory | Management are advised to review procurement policies and procedures and mode contract language to ensure that those engaging with the Council are contractually obligated to comply with the Council's information management standards. | Head of Procurement<br><br>**Target date:**<br><br>30 September 2015 |

# Appendix 1 – Basis of our classifications

### Individual finding ratings

| Finding rating | Assessment rationale |
|---|---|
| Critical | A finding that could have a:<br>• ***Critical*** impact on operational performance; or<br>• ***Critical*** monetary or financial statement impact; or<br>• ***Critical*** breach in laws and regulations that could result in material fines or consequences***;*** *or*<br>• ***Critical*** impact on the reputation or brand of the organisation which could threaten its future viability. |
| High | A finding that could have a:<br>• ***Significant*** impact on operational performance; or<br>• ***Significant*** monetary or financial statement impact ; or<br>• ***Significant*** breach in laws and regulations resulting in significant fines and consequences ***;*** *or*<br>• ***Significant*** impact on the reputation or brand of the organisation. |
| Medium | A finding that could have a:<br>• ***Moderate*** impact on operational performance; or<br>• ***Moderate*** monetary or financial statement impact; or<br>• ***Moderate*** breach in laws and regulations resulting in fines and consequences; or<br>• ***Moderate*** impact on the reputation or brand of the organisation. |
| Low | A finding that could have a:<br>• ***Minor*** impact on the organisation's operational performance; or<br>• ***Minor*** monetary or financial statement impact; or<br>• ***Minor*** breach in laws and regulations with limited consequences; or<br>• ***Minor*** impact on the reputation of the organisation. |
| Advisory | A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice. |

## Report classifications

| Findings rating | Points |
|---|---|
| Critical | 40 points per finding |
| High | 10 points per finding |
| Medium | 3 points per finding |
| Low | 1 point per finding |

| Report classification | Points |
|---|---|
| Low risk | 6 points or less |
| Medium risk | 7– 15 points |
| High risk | 16– 39 points |
| Critical risk | 40 points and over |

# Appendix 2 – Agreed Terms of reference

## Background

The Public Records (Scotland) Act 2011 requires Local Authorities to prepare and implement a records management plan (RMP) which sets out proper arrangements for the management of records. Aberdeen City Council is required to submit the plan to the Keeper of the Records of Scotland in November 2014.

A model plan which includes 14 elements has been developed by the "Keeper" to illustrate best practice. The Council is required to include all 14 elements within the submission or confirm that the element is not applicable, providing an explanation for the omission. The 14 elements, included within the model plan, are as follows:

- Senior management responsibility
- Records manager responsibility
- Records management policy statement
- Business classification
- Retention schedules
- Destruction arrangements
- Archiving and transfer arrangements
- Information security
- Data protection
- Business continuity and vital records
- Audit trail
- Competency framework for records management staff
- Assessment and review
- Shared information

As per the “assessment and review” element it is required that the operating effectiveness of the plan is assessed after implementation. To ensure this can be achieved management must develop an appropriate programme of controls testing.

In preparation for completing of the RMP, a business plan has been produced by the Records Manager.

# Scope

Internal Audit’s review of the Public Records (Scotland) Act will consist of two phases of fieldwork. Both phases will be reported to Audit and Risk Committee in December 2014.

| Phase | Objectives | Period | Days allocated |
|---|---|---|---|
| I | Review the RMP Business Plan to ensure:<br><br>a) “Completed” tasks meet best practice (as detailed within the Keeper of the Records of Scotland Model Plan) and there is evidence to support that tasks have been completed as described.<br><br>b) “Un-completed” tasks have an action plan in place, timescales are appropriate and the intended actions meet best practice (as detailed within the Keeper of the Records of Scotland Model Plan) | 05 August – 11 August 2014 | 5 |
| II | Assess the design of the programme of controls testing, providing recommendations where improvements could be made. | TBC | 5 |

# Limitations of scope

The scope of our review is outlined above.

Internal control, no matter how well designed and operated, can provide only reasonable and not absolute assurance regarding achievement of an organisation's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

# Audit approach

Our audit approach is as follows:

- Obtain an understanding of the procedures in place through discussion with key personnel and review of documentation.
- Identify the key risks in respect of compliance with the Public Records (Scotland) Act.
- Review the Council's RMP Business Plan against best practice guidance (model plan).
- Evaluate the design of controls in place to assess compliance with the RMP.

# Appendix 3 – Limitations and responsibilities

## Limitations inherent to the internal auditor's work

We have undertaken a review of Compliance with the Public Records (Scotland) Act, subject to the limitations outlined below.

## Internal control

Internal control, no matter how well designed and operated, can provide only reasonable and not absolute assurance regarding achievement of an organisation's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

## Future periods

Our assessment of controls relating to Compliance with the Public Records (Scotland) Act is as at April 2015 (Phase 2). Historic evaluation of effectiveness is not relevant to future periods due to the risk that:

- the design of controls may become inadequate because of changes in operating environment, law, regulation or other; or
- The degree of compliance with policies and procedures may deteriorate.

## Responsibilities of management and internal auditors

It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.

We endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we shall carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected.

Accordingly, our examinations as internal auditors should not be relied upon solely to disclose fraud, defalcations or other irregularities which may exist.