



INTERNAL AUDIT, RISK & COMPLIANCE SERVICES

Argyll & Bute Council  
Internal audit report – Risk management  
22 June 2009

Report Number 004

This report is CONFIDENTIAL and its circulation and use are restricted – see notice on page 2

**ADVISORY**

# Contents

Executive summary.....	3
Internal audit findings to be actioned .....	5
Appendix 1 – Objective, scope and approach.....	12
Appendix 2 – Classification of internal audit findings .....	13

## Distribution

### For action

Iain Jackson	Governance & Risk Manager
Charles Reppke	Head of Democratic Services and Governance

### For information

The chair and members	Audit Committee
Bruce West	Head of Strategic Finance
Ian Nisbet	Internal Audit Manager

*This report has been prepared on the basis set out in our internal audit services contract with Argyll & Bute Council (the client), dated 22 January 2009, in respect of internal audit services, and should be read in conjunction with the contract. This report is for the benefit only of the client and the other parties that we have agreed in writing to treat as addressees of the engagement letter (together the beneficiaries), and has been released to the beneficiaries on the basis that it shall not be copied, referred to or disclosed, in whole or in part, without our prior written consent. Nothing in this report constitutes a valuation or legal advice. We have not verified the reliability or accuracy of any information obtained in the course of our work, other than the limited circumstances set out in the engagement letter. This report is not suitable to be relied on by any party wishing to acquire rights against KPMG LLP (other than the beneficiaries) for any purpose or in any context. Any party other than the beneficiaries that obtains access to this report or a copy and chooses to rely on this report or a copy (under the Freedom of Information (Scotland) Act 2002 or otherwise and chooses to rely on this report (or any part of it) does so at its own risk. To the fullest extent permitted by law, KPMG LLP does not assume any responsibility and will not accept any liability in respect of this report to any party other than the beneficiaries.*

# Executive summary

## Summary of objective and scope

As part of the 2008-09 internal audit plan, as approved by the audit committee of Argyll and Bute Council (“the Council”), an internal audit review of the risk management process was performed in March 2009.

The overall objective of this review was to consider the processes and controls within the Council to manage risk. The project focused upon the risk management framework within the Council. The internal audit did not consider the appropriateness of risks included within risk registers.

The specific objective, scope and approach in respect of this internal audit are detailed in Appendix 1.

## Background

The Council has historically maintained a strategic risk register, capturing all risks identified from directorate Loss Control Groups (“LCG”) and the corporate level risk management group (“RMG”). Responsibility for facilitating the risk management process is assigned to the Council’s governance and risk manager.

While risk management processes have been established within the Council for a number of years the recent appointment of the new chief executive has re-invigorated the process and the importance of effective risk management. This has resulted in a series of initiatives including:

- re-visiting the strategic risk register to refresh the risks identified and re-assessing the potential impact of the risks over the delivery of the Council’s corporate plan;

- the creation of an operational risk register for each of the 13 service lines within the Council. Heads of service have been allocated responsibility for their own operational risk registers; and
- the updating, in January 2009, of the Council’s risk management policy statement and risk management strategy. These are currently awaiting final approval.

The consideration of risk has also been integrated into the Council’s business planning processes. This was evident in the current corporate plan development process and in the development of the 2009-10 revenue budgets.

## Key findings and recommendations

The findings identified during the course of this internal audit are summarised below. A full list of the findings and recommendations are included in this report. Classification of internal audit findings are detailed in Appendix 2.

	High	Medium	Low
Number of internal audit findings	3	2	1

These findings and recommendations were discussed with management who have accepted the findings and have agreed actions to address the recommendations.

The intention of this review was to take advantage of the existing momentum and to raise the profile of the importance of effective risk management within the Council. In addition, the aim was to build upon the existing structures and processes already established.

## Executive summary

### Summary of internal audit findings

Ref #	Description of internal audit findings	Rating of internal audit findings			Target date
		High	Medium	Low	
1	<b>Risk management policy and framework:</b> The risk management policy and risk management framework document would benefit from updating to reflect the ongoing development of the risk management process within the Council. Once updated this should be approved by the strategic management team and the Council.				31 October 2010
2	<b>Oversight and Challenge:</b> The governance responsibilities for risk management have yet to be fully and clearly defined across the organisation, including to all relevant individuals and groups involved within the risk management process.				31 October 2010
3	<b>Risk identification and assessment:</b> The existing risk identification and assessment process should be further developed to provide clear and transparent guidance for all stakeholders.				31 October 2010
4	<b>Risk aggregation:</b> The risk aggregation process has yet to be clearly defined to ensure the effective aggregation of risks from 13 operational risk registers into one strategic risk register.				31 October 2010
5	<b>Risk monitoring and reporting:</b> No formal risk reporting process has yet been developed, however, ongoing developments with Pyramid are acknowledged.				31 October 2010
6	<b>Communication and change:</b> No road map or implementation plan exists to improve and develop the existing risk management process.				31 October 2009

## Internal audit findings to be actioned

### 1. Risk management policy and framework

**Rating of internal audit finding:  
 Medium**

Finding(s) and impact	Recommendation(s)	Agreed Management action(s)
<p>Whilst the current documents have provided a firm basis on which to progress the risk management policy statement and risk management strategy, these should be updated to ensure that they are prescriptive and contain a clear and comprehensive risk management process.</p>	<p>1) Management should implement a risk management framework supported by a risk management policy. The recommendations outlined within the remainder of the risk management report should be reflected in the revised documentation. Once finalised, management should ensure the risk management policy and framework is approved by the strategic management team and Council. Management should ensure that the risk management policy includes the following elements, including:</p> <ul style="list-style-type: none"> <li>• a clear statement of risk management vision and value for the Council by the chief executive;</li> <li>• a high level outline of the Council's approach, appetite for risk and approach to risk management;</li> <li>• reference to any legal requirements for policy statements; and</li> <li>• links to the planning performance groups, community planning partnership, business continuity planning and single outcome agreement. Risk management should then be mirrored to ensure risk framework and processes are effective across the wider organisation.</li> </ul> <p>2) Management should develop a risk management framework document to support the risk management policy by providing a set of tools and techniques. Management should consider the inclusion of the following</p>	<p><b>Action:</b></p> <p>1 &amp; 2. Agreed. This will form a key milestone within the road map to be developed.</p> <p><b>Responsibility:</b> Iain Jackson</p> <p><b>Target Date:</b></p> <p>Road Map – 31 October 2009</p> <p>Completion Date – 31 October 2010 (all actions identified on road map).</p>

	<p>sections when developing the risk management framework to ensure clear understanding of the end to end process:</p> <ul style="list-style-type: none"><li>• document revision history;</li><li>• ownership, review and approval;</li><li>• contact information;</li><li>• introduction (i.e. objectives, benefits, application, risk management process);</li><li>• risk identification;</li><li>• risk assessment;</li><li>• risk mitigation;</li><li>• risk monitoring and reporting;</li><li>• governance responsibilities; and</li><li>• appendices (i.e. example risk register, example risk reporting, glossary of terms).</li></ul>	
--	---	--

**2. Oversight and challenge**

**Rating of internal audit finding:  
 High**

Finding(s) and impact	Recommendation(s)	Agreed Management action(s)
<p>While acknowledging that the risk management policy statement and strategy has recently been updated (January 2009), we have identified further opportunities for enhancement, by, for example, including:</p> <ul style="list-style-type: none"> <li>• the overall risk governance structure and the roles of the different elements of the Council’s arrangements in risk management; and</li> <li>• specific details of responsibility for ownership, review and approval of risk registers.</li> </ul> <p>As part of this review, we discussed the risk governance structure and roles in terms of the risk management process with a broad cross section of management. We found that there appears to be inconsistent views in relation to the purpose, role and responsibilities of some groups involved in the existing risk management process:</p> <ul style="list-style-type: none"> <li>• senior management team;</li> <li>• risk management group;</li> <li>• department management team meetings; and</li> <li>• loss control groups.</li> </ul> <p>The absence of clarity and understanding of the risk management governance process increases the risk of a less effective and efficient risk management process. In addition, it also reduces the likelihood of actions being implemented and monitored appropriately.</p>	<ol style="list-style-type: none"> <li>1) Management should ensure that the risk management framework clearly defines the overall risk governance structure together with the role of the different elements of the Council’s management arrangements.</li> <li>2) Management should ensure that terms of reference for all groups within the Council are clearly outlined, including their responsibilities and role in terms of the risk management process.</li> <li>3) Information on the roles and responsibilities in respect of the risk management governance process should be clearly outlined within the Council’s risk management framework.</li> </ol>	<p><b>Action:</b></p> <p>1, 2 &amp; 3. Agreed. This will form a key milestone within the road map to be developed.</p> <p><b>Responsibility:</b> Iain Jackson</p> <p><b>Target Date:</b></p> <p>Road Map – 31 October 2009</p> <p>Completion Date – 31 October 2010        (all actions identified on road map)</p>

**3. Risk identification and assessment**

**Rating of internal audit finding: High**

Finding(s) and impact	Recommendation(s)	Agreed Management action(s)
<p>There is currently no detailed guidance that describes the risk identification and assessment process within the Council. The current risk management policy statement gives high level guidance, however it does not give insight to how the strategic or operational risk registers should be populated or describes how a risk should be defined. This guidance would generally be documented within a risk framework policy and used to communicate and develop understanding of the risk management process throughout the organisation.</p> <p>The absence of this detailed guidance may increase the risk of incorrect risks being identified or significant risks not being identified. It may also reduce the efficiency of the risk management process. The effective identification and capture of risks is a critical component of an effective risk management process. We noted that the risk management group has to date been responsible for ensuring that there has been a consistent approach to risk identification and assessment, however, management accepted that more detail guidance would be beneficial.</p> <p>The strategic risk registers, and more recently, the operational risk registers were reviewed and found to contain a number of the key components expected to be present. However, there remains some scope for improvement and development in terms of sophistication. The strengthening of the risk register template will enhance the understanding of the individual risks and the controls associated with risk mitigation.</p>	<p>1) Management should modify existing documentation to develop a risk management framework. This framework should defined the following elements:</p> <ul style="list-style-type: none"> <li>• guidance on how to identify and assess risks;</li> <li>• clearly define the parameters of the risk register;</li> <li>• contain an example risk register containing a risk documented using best practice; and</li> <li>• define the risk register review process and timetable.</li> </ul> <p>2) Management should consider updating the existing risk register templates in order to strengthen their role as a tool within the risk management process. The update should include the following enhancements:</p> <ul style="list-style-type: none"> <li>• risk description and controls should be more prescriptive;</li> <li>• causes and consequences of each risk should be made explicit;</li> <li>• risk score (likelihood x impact) should be included;</li> <li>• opportunities and positive impacts of risks described;</li> <li>• risk classification</li> <li>• linking KPI's (or PIs) to each risk where appropriate; and</li> <li>• status update for risk actions and timescale for risk action should be specific and measureable.</li> </ul>	<p><b>Action:</b></p> <p>1 &amp; 2. Agreed. This will form a key milestone within the road map to be developed.</p> <p><b>Responsibility:</b></p> <p>Iain Jackson</p> <p><b>Target Date:</b></p> <p>Road Map – 31 October 2009</p> <p>Completion Date – 31 October 2010 (all actions identified on road map)</p>



**4. Risk aggregation**

**Rating of internal audit finding:  
 Medium**

Finding(s) and impact	Recommendation(s)	Agreed Management action(s)
<p>The Council has recently revisited the strategic risk register to refresh the risks previously identified. In addition, it has also instigated the creation of an operational risk register for each of the 13 service lines within the Council.</p> <p>Whilst this is a positive development, consideration still requires to be given as to how the operational risks within the 13 service lines will be distilled into a single strategic risk register for the Council. The aggregation or distillation process is important to ensure that the appropriate risks are captured to a single point allowing the Council members and senior management team to understand the most prominent risks or themes affecting the Council at any one time.</p> <p>To support the distillation process a formal risk appetite should be defined by the Council. This appetite can be defined by determining the level of risk that would engage an escalation process. This is where an issue or event of sufficient gravity should arise that it needs to be communicated to the Council members immediately. This will allow the organisation to understand the 'appetite' of the Council in terms of risk and ensure critical risks are escalated to the appropriate level within the organisation.</p>	<ol style="list-style-type: none"> <li>1) Management should embed a risk aggregation process within the organisation that defines how risks from the 13 operational risks registers are recorded and distilled onto the strategic risk register.</li> <li>2) Management should define the risk appetite for the Council within the risk management framework document and referenced within the risk management policy.</li> </ol>	<p><b>Action:</b></p> <p>1 &amp; 2. Agreed. This will form a key milestone within the road map to be developed.</p> <p><b>Responsibility:</b></p> <p>Iain Jackson</p> <p><b>Target Date:</b></p> <p>Road Map – 31 October 2009</p> <p>Completion Date – 31 October 2010        (all actions identified on road map)</p>

**5. Risk monitoring and reporting**

**Rating of internal audit finding:  
Low**

Finding(s) and impact	Recommendation(s)	Agreed Management action(s)
<p>Risk reporting within the Council has not yet been defined however, we have been advised that risk reporting will be incorporated within the 'Pyramid' performance management tool.</p> <p>It was acknowledged that this was an area of ongoing development and that the establishment of a more embedded risk management process is a high priority.</p>	<ol style="list-style-type: none"> <li>1) Management should consider the process for refining the risk reporting process and outputs to ensure risk reports contain relevant, transparent and reliable data.</li> <li>2) The risk reporting process and examples of effective risk reporting should be documented within the risk management framework guidance.</li> </ol>	<p><b>Action:</b> 1 &amp; 2. Agreed. This will form a key milestone within the road map to be developed.</p> <p><b>Responsibility:</b> Iain Jackson</p> <p><b>Target Date:</b> Road Map – 31 October 2009 Completion Date – 31 October 2010 (all actions identified on road map)</p>

**6. Communication and change**

**Rating of internal audit finding:  
 High**

Finding(s) and impact	Recommendation(s)	Agreed Management action(s)
<p>The profile of risk management within the Council has been increased in recent months, most notably with risk forming an integrated part of the business planning process to develop the new corporate plan and budgets for the Council. To date management have not yet developed a road map to define the ultimate aim for Council in terms of risk management and the milestones that need to be achieved in order to reach this objective. In addition, an engagement and communication plan for staff and other stakeholders to support this implementation has not been formally considered.</p> <p>The creation of a road map supported by an engagement and communication plan would enhance the potential value the Council will receive from an embedded risk management process. It will also ensure employees appreciate and understand the value linked to this process.</p>	<p>1) Management should develop a road map that defines the ultimate objective for the Council in terms of risk management process and determine that appropriate milestones and resources are allocated to support delivery.</p> <p>2) Following the approval of an updated risk management policy and framework document, management should formulate and implement an engagement and communication plan to ensure all employees understand and see value in the risk management process adopted by the Council. The plan should consider the following elements:</p> <ul style="list-style-type: none"> <li>• what information is to be communicated;</li> <li>• who will communicate the information, i.e. what roles the respective groups and sub-committees will have in the communication process;</li> <li>• when the information is to be communicated;</li> <li>• a risk management contact to approach with any questions; and</li> <li>• a training timetable.</li> </ul>	<p><b>Action:</b></p> <p>1 &amp; 2. Agreed.</p> <p>The road map will incorporate all the points highlighted in this report identifying milestone completion dates that reflect the rating given to the individual findings.</p> <p><b>Responsibility:</b> Iain Jackson</p> <p><b>Target Date:</b></p> <p>Road Map – 31 October 2009</p> <p>Completion Date – 31 October 2010 (all actions identified on road map)</p>

## Appendix 1 – Objective, scope and approach

As part of the 2008-09 internal audit plan, as approved by the audit committee of the Council (“the Council”), an internal audit review of the risk management will be performed in March 2009.

### Objective

To consider the processes and controls in place to manage risk.

### Scope

Based on the objective outlined above, the scope of the review was to:

- consider whether a risk management process existed;
- consider the controls and processes established to ensure effective risk management can be implemented;
- consider the controls and processes established to monitor compliance with risk management;
- identify the processes to communicate risk management;
- identify the processes adopted to manage risk management;
- identify policies and procedures and determine how compliance is monitored; and
- on a sample basis, test compliance with the identified policies and procedures.

### Exclusions

The project did not consider the appropriateness of risks included in risk registers.

### Approach

The internal audit was conducted by holding discussions with key members of Council staff and considering available documentation. Key staff members with whom we held discussions included:

- Sally Reid, Chief Executive
- Nigel Stewart, Corporate Services Director
- Andrew Law, Operational Services Director
- Charles Reppke, Head of Democratic Services and Governance
- Lyndis Davidson, Policy and Strategy
- Ernie Brown, Health and Safety and Training Manager, Community Services
- Donald MacVicar, Head of Planning and Performance, Community Services
- Ian Nisbet, Internal Audit Manager
- Dave Tomlinson, Support Services Manager, Development Services
- Terry Markwick, Central Services Manager, Operational Services
- Tom MacFarlane, Principle Resource and Quality manager, Operational Services

## Appendix 2 – Classification of internal audit findings

The following framework for internal audit ratings has been developed and agreed with management for prioritising internal audit findings according to their relative significance depending on their impact to the process. The individual internal audit findings contained in this report have been discussed and rated with management.

Rating	Definition
<b>High</b>	<p>Observations on high level controls and other important internal controls. Significant matters relating to factors critical to the success of the objectives of the system.</p> <p>The weakness may therefore give rise to loss or error</p>
<b>Medium</b>	<p>Observations on less important internal controls, improvements to the efficiency and effectiveness of controls which will assist in meeting the objectives of the system and items which could be significant in the future.</p> <p>The weakness is not necessarily great, but the risk of error would be significantly reduced if it were rectified</p>
<b>Low</b>	<p>Observations to improve the efficiency and effectiveness of controls, one-off items subsequently corrected.</p> <p>The weakness does not appear to affect the ability of the system to meet its objectives in any significant way</p>