Argyll & Bute Council

Review of Risk Management Arrangements

Gary Devlin
Engagement Lead
T: 0131 659 8554
E: gary.j.devlin@uk.gt.com

Grace Scanlin
Senior Manager
T: 0131 659 8526
E: grace.scanlin@uk.gt.com

Contents

1	**Executive Summary**	**1**
2	**Detailed Findings**	**4**

Appendices

A	**Risk Maturity Assessment**	**6**
B	**Definition of internal audit ratings**	**11**

1 Executive Summary

1.1 Background

Effective risk management is a key element of the Council's overall governance arrangements. We agreed with the Audit Committee that we would review the Council's risk management arrangements with two key objectives:

- to assess the maturity of risk management arrangements to inform our audit strategy
- to review the evolving risk management approach and make recommendations for further improvement.

The Council's Audit Committee has the responsibility to review the effectiveness of risk management systems, and for ensuring that management is addressing key strategic risks. The Performance Review and Scrutiny Committee also considers risk management arrangements, in line with their role in scrutinising performance against strategic and corporate objectives.

Responsibility for risk management is delegated to the Strategic Management Team (SMT), with responsibility for risk management led by the Head of Strategic Finance. The Council has established a Strategic Risk Group comprising of the Chief Executive, Executive Directors, and representatives from Emergency Planning, Governance and Law, Improvement and HR, and Strategic Finance. This Group plays a key role in reviewing and assessing risks across the Council, and the mitigating actions to respond.

1.2 Audit Approach

Our review considered the way in which risk is managed at the Council, drawing on a risk maturity assessment tool (Appendix 2). We undertook a desktop exercise which reviewed terms of reference, the risk management policy and guidance, committee reports on the strategic risk register and the operational risk registers prepared by a sample of departments. We also reviewed the risk monitoring facilities on the Council's performance monitoring system, Pyramid. Interviews were undertaken with key contacts, including the Head of Strategic Finance and Risk Manager (see Appendix 1).

We considered the following risks as part of the review:

- roles and responsibilities at Committee and Executive level may not be clear, leading to confusion over lines of accountability
- the risk management process is not fit for purpose, meaning that the Council is not managing risk effectively
- risk may not be given sufficient priority by individuals and groups managing it, meaning that risks are poorly understood and addressed.

We did not consider the content of the risk register, nor consider in detail the process for managing operational risk.

1.3 Key findings

Assessment of risk maturity: Risk Managed

The first stage of risk based auditing is to assess the level of risk maturity within the Council. This allows us to determine our audit strategy, in line with guidelines from the Institute of Internal Auditors (IIA). The IIA define five stages of risk maturity (Table 1, below). We used an assessment tool based on IIA guidance "An approach to implementing Risk Based Auditing" and the HM Treasury's Risk Management Assessment Framework.

Table 1: Stages of Organisational Risk Maturity

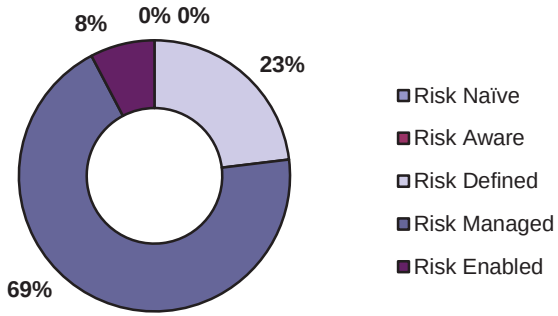
Stage	Key characteristics
Risk Naïve	No formal approach developed for risk management
Risk Aware	Scattered silo based approach to risk management
Risk Defined	Strategy and policies in place and communicated
Risk Managed	Council wide approach to risk management developed and communicated
Risk Enabled	Risk management and internal control fully embedded in the operations of the Council

Our detailed assessment is attached at Appendix 2, which assesses risk management practices against six categories:

- Leadership
- Risk strategy and policies
- Processes
- People
- Risk Handling
- Outcomes.

Figure 1, below outlines our assessment against the risk maturity questionnaire. Overall we found that risk management arrangements are well-developed and continue to embed across the Council. Plans are in place to ensure that arrangements continue to improve through, for example, participation in self-assessment exercises and CIPFA's benchmarking group. Improvements are logged in the Risk Management Action Plan. There were no areas where we assessed arrangements as risk naïve or risk aware.

Figure 1: Risk Maturity Assessments (Appendix 1)



During interviews, officers were confident that the key risks facing the Council are identified and monitored. Our assessment highlighted two potential areas for improvement, relating to the Council's definition of risk appetite, and consideration of the opportunities, or positive emerging risks.

Audit Opinion: Substantial

Our detailed findings in Section 2 identify 3 recommendations, which are intended to continue to improve the Council's overall risk management arrangements.

Level of Assurance	Reason for the level of Assurance given
High	Internal Control, Governance and the Management of Risk are at a high standard with only marginal elements of residual risk, which are either being accepted or dealt with.
Substantial	Internal Control, Governance and the Management of Risk have displayed a mixture of little residual risk, but other elements of residual risk that are slightly above an acceptable level and need to be addressed within a reasonable timescale.
Limited	Internal Control, Governance and the Management of Risk are displaying a general trend of unacceptable residual risk and weaknesses must be addressed within a reasonable timescale, with management allocating appropriate resource to the issues.
Very Limited	Internal Control, Governance and the Management of Risk are displaying key weaknesses and extensive residual risk above an acceptable level which must be addressed urgently, with management allocating appropriate resource to the issues.

1.4 Overall Conclusions

Overall, at officer level, we found a good level of understanding about the risk management process, and clear engagement about new and emerging risks.

Ultimately, Council members are responsible for managing risks effectively. Member seminars have been held to review and agree the Strategic Risk Register. We hope that work to map sources of assurance relating to Strategic Risks will identify any areas of duplication or lack of clarity relating to accountability for risk management.

1.5 Acknowledgement

Our audit involved discussions with a range of individuals across the Council, including the Risk Manager and Heads of Service. We would like to take this opportunity to thank those staff for their assistance and co-operation during the course of the audit.

2 Detailed Findings

1.	Medium	Risk prioritisation

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
The most recent Strategic Risk Register identifies 15 risks with gross risk scores ranging between 9 – 20, and residual risks classing 14 of the risks as 'amber' and one, relating to population and economic decline as a 'red' risk. Each of the risks is currently managed in the same way, with mitigation actions and planned actions reported to the Strategic Risk Group and Committees in the SRR. However, where risks remain 'red,' or above the risk appetite level we would recommend escalation of the risk to give management and the Audit Committee additional assurance that risks are being managed effectively.	We propose that where strategic risks remain 'red' after current mitigation measures: ▪ Action plans are produced to document owners and expected timescales (including long and medium term measures) for mitigating actions to become effective. ▪ Risk owners should be available to explain progress against risks to the Audit Committee or Performance Review and Scrutiny Committee, where requested.	Strategic Risk Group will review protocols considering proposed actions. A number of mitigations are already subject to delivery /realisation monitoring arrangements Date Effective: February 2015 Owner: Bruce West

.

2.	Medium	Risk appetite

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
The Council's current approach to defining the risk appetite for each strategic risk to use the residual risk scores from when the SRR was reviewed as a proxy. A more formal approach to defining risk appetite would mean that the Council could : ▪ use the gap between the current residual risk score and risk appetite to prioritise actions ▪ clarify areas where risks cannot fully be managed by the Council, eg population decline ▪ demonstrate the journey of improvement across individual risk categories ▪ acknowledge a willingness to take on risk in individual cases, where there is potential benefit to the Council to do so.	We propose that the Council's Strategic Risk Group facilitates initial discussions on risk appetite levels for individual risks, and develops a framework for monitoring progress.	Strategic Risk Group will lead developments on Risk Appetite and associated monitoring / mapping frameworks Date Effective: Feb 2015 Owner: Bruce West

3.	Information	Opportunities

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
The Council's Risk Management Guidance for Services focuses on identifying both risks and opportunities that may impact on the achievement of Council objectives. However, in practice, we noted that most formal risk management within the SRR and ORRs focused on 'negative' risks, where there is a threat to the Council's objectives.	We recommend that update reports on the Strategic Risk Register should include a section on emerging opportunities, to ensure that risk management arrangements support informed decision-making.	SRG will consider Emerging Opportunities / positive risk and agree appropriate reporting mechanisms. Date Effective: 31 March 2015 Owner: Bruce West

A Risk Maturity Assessment

		Risk Naïve		Risk Aware		Risk Defined		Risk Managed		Risk Enabled
Key characteristics:		**No formal approach developed for risk management**		**Scattered silo based approach to risk management**		**Strategy and policies in place and communicated**		**Council wide approach to risk management developed and communicated**		**Risk management and internal control fully embedded in the Council's operations**
Category:		Explanation of risk maturity level								
Leadership										
How are the organisation's objectives identified and defined? Who are they communicated to?		No formal objectives set. No guidance on risk management offered		Objectives defined, but a process cannot be evidenced. Only senior staff have knowledge of objectives. Risk management encouraged but no guidance given		Objectives defined and agreed by the Board. Some staff aware of objectives. Some risk management guidance offered by senior management		Objectives defined following a review of the organisation. Staff are aware of the objectives. Senior management have developed and communicated risk management guidance to key people		Rigorous objective setting and risk management process occurs periodically. The output is fully embedded in the organisation and communicated to all staff

	Risk Naïve	Risk Aware	Risk Defined	Risk Managed	Risk Enabled
How has the risk appetite of the organisation been defined? How does this operate in practice? What is the organisational culture in terms of risk management?	No risk appetite in place. Risk management practices are reliant upon individual integrity.	No formal risk appetite in place but a cultural philosophy is in place. Risk management championed by a senior member of the organisation.	Risk appetite defined in risk methodology, but management apply common sense approach to the application. Board discuss risks as per management's views.	Risk appetite defined in terms of the risk scoring methodology and applied in practice to identify risks in need of further management. Board empower managers with risk management processes but retain oversight.	Risks outside of the risk appetite escalated to the right level of the organisation and decision making process is evidenced through debate. Board champion risk management and drive change through this.
Risk strategy and policies					
How has the strategy of the organisation in terms of risk management been identified and created?	No strategy for risk management in place	No formal strategy in place but a cultural philosophy is present (ie single person's approach communicated)	Documented strategy links to objectives but not developed in consultation with others	Strategy developed through analysis of existing arrangements and Council approved	Detailed strategy developed via consultation from across the organisation. Live document
How is the risk management strategy and/or policy applied in practice?	No strategy or policy in place or not applied	Strategy and/or policy verbally communicated but application not monitored	Application of documented strategy and/or policy by management	Strategy implemented by departmental instruction to other staff members	Staff engaged in strategy development and implementation. Everyone 'owns' the strategy

	Risk Naïve	Risk Aware	Risk Defined	Risk Managed	Risk Enabled
People					
How has the organisation ensured that its people are aware of risk management tools and techniques?	No training provided	Limited training provided	Training has been provided on understanding risks	Training has been provided on risk management strategies and ownership	Training is ongoing, with regular updates across the organisation and new methodologies being applied where relevant.
Who is responsible for risk management within the organisation?	One individual	Senior management	Individuals from across the organisation and management	Groups within each function in combination with management	All staff
Processes					
What process has been followed to identify and record risks?	Reactive responses to risks as they occur, no formal logging	Individual identification and logging of risks in own area	Key risks identified, logged and communicated in a consistent manner	Defined process followed to identify and log risks, all parts of organisation involved. Opportunities also part of process	Fundamental part of all activities, including projects. Risks identified, logged and ranked as matter of course, opportunities regularly being identified
What scoring system is used to assess risks? How is this applied in practice?	No scoring system	Some scoring occurs but not consistently applied across the organisation	Standard scoring process applied to corporate risks, but not across the organisation	Defined process for scoring risks that is consistently applied	Process is used to drive change - scoring is challenged and live

		Risk Naïve		Risk Aware		Risk Defined		Risk Managed		Risk Enabled
How have responses to the risks been identified (eg controls in the risk register), selected and implemented?		No responses to risks identified		Responses not documented but applied in a reactive manner		Responses documented and assessed for adequacy. Management rely upon othesr to implement actions		Responses selected based upon the need to the organisation. Assurance obtained that responses operating effectively.		Responses identified and implemented as the risk is identified. Assurance built into the controls. Staff identify and implement responses timely
What methods/controls are in place to review risks and monitor the operation of key controls?		None or management rely upon nothing bad happening		Risk logging is isolated and poorly reviewed. Some controls operate without any monitoring, whilst others are tested periodically.		Key risks are logged but rarely reviewed. Controls are monitored on a periodic basis, either through testing or reviews by audit		Risks are logged and regularly reviewed. Controls monitored regularly and assurance sought		Risks logged, ranked and live. Owners champion mitigation and controls. Controls monitored in line with importance. Assurance provided as a matter of course
Risk Handling										
How are risks reviewed by the organisation/audit unit? How often does this take place?		No formal review of risks		Some risks are reviewed, but infrequently		Risks are reviewed on a periodic basis by risk owners. Limited documentation		Risks are reviewed in consultation with others to meet the needs of the organisation and documentation exists		Risks are live, continuously reviewed and communicated across the organisation,

	Risk Naïve	Risk Aware	Risk Defined	Risk Managed	Risk Enabled
What evidence is there that risk management is effectively operating within the organisation? How is it evidenced in decision making?	Reliance placed on no risks crystallising	Management review risk management activities periodically, generally not in conjunction with relevant decision-making	Management required to report on risk management activity periodically and review new decisions in its light	Risk management integrated into decision making, assurance sought from one source and actions addressed	Risk management drives decision making, assurance actively sought from a variety of sources and improvement continuous
Outcomes					
How is risk management built into performance management processes?	Risk management exists in isolation	Performance reviews do not consider risk management unless major issue has arisen	Periodic reviews of performance include assessment of negative risk management performance	Periodic reviews of performance include assessment of positive and negative risk management performance	Continuous assessment of risk management performance, both positive and negative. Risks drive performance assessment
How well has the organisation achieved its desired outcomes? How much of this is attributed to effective risk management?	No outcomes achieved	Unknown risks materialised preventing outcomes being achieved or outcomes achieved due to luck rather than judgement	Some outcomes achieved, but some surprises present	Risk management believed to play a part in achieving all outcomes but cannot be evidenced as such	Risk management clearly demonstrates how outcomes have been achieved and is a primary reason

B Definition of internal audit ratings

Audit issue rating

Within each report, every audit issue is given a rating. This is summarised in the table below.

Rating	Description	Features	Report rating indicators
High	Findings that are fundamental to the management of risk in the business area, representing a weakness in control that requires the immediate attention of management	• Key control not designed or operating effectively • Potential for fraud identified • Non compliance with key procedures / standards • Non compliance with regulation	• Multiple critical issues identified • Previously agreed actions of critical issues have not been addressed
Medium	Important findings that are to be resolved by line management.	• Impact is contained department and compensating controls would detect errors • Possibility for fraud exists • Control failures identified but not in key controls • Non compliance with procedures / standards (but not resulting in key control failure)	• Multiple important issues identified • Partial completion of previously agreed actions
Low	Findings that identify non-compliance with established procedures.	• Minor control weakness • Minor non compliance with procedures / standards	• No more than two important issues identified or multiple advisory issues • Minor previously agreed actions not completed
Information	Items requiring no action but which may be of interest to management or best practice advice	• Information for department management • Control operating but not necessarily in accordance with best practice	• Issues identified are only best practice in nature

www.grant-thornton.co.uk