# RISK MANAGEMENT STRATEGY

INTRODUCTION

The management of risk is a crucial aspect of internal control and therefore a key element of good governance in any organisation. "Governance" is a well recognised term but an often mis-understood concept. Many people see it simply as the rules and controls in place within an organisation (sometimes perceived as barriers to activity) but it is in fact much broader; it encompasses the culture, leadership, values, systems, processes, controls and resources and more importantly, how these are directed and managed to enable the organisation to achieve its objectives and defined outcomes. Far from being a barrier to getting things done, good governance is the key enabler for success.

To be effective, any risk management process must create value by increasing the ability or likelihood of achieving aims and objectives. In the context of local government, robust risk management creates value through facilitating better decision making, more effective internal control, service improvement, change and innovation. To achieve this however, the management of risk and the setting of controls must be directly linked to the priorities and objectives of the Council, integrated into all of our business processes and implemented consistently across the whole organisation.

Many organisations, across all sectors, make the mistake of treating risk management as a compliance driven, stand-alone function; perceived as "centrally" owned and somewhat detached from day-to-day operations. This approach undermines the ability of these organisations to derive the most value from the risk management processes. Risk reporting and monitoring becomes too resource intensive and complex and as a result the organisation has no comprehensive oversight of its risks. In many organisations the process of risk reporting and monitoring ends up being the output as opposed to the means to an end; that end being increasing the likelihood of the organisation achieving its objectives.

Whilst the language around risk may be technical at times, integrated risk management as a concept is relatively straightforward and highly effective, if applied consistently and at every level throughout the organisation. Key to effective integrated risk management is the direct link of the controls to the objectives (as illustrated in figure 1). In summary;-

- What is it that you are trying to achieve? (business objective/aim/outcome)
- What is likely to prevent or hinder you from achieving that objective? (risk event)
- In those circumstances, what do you need the control to do to help eliminate or mitigate the risk? (the control objective)
- Develop, test, monitor and review the control to ensure that it is effective (key control)

Figure 1
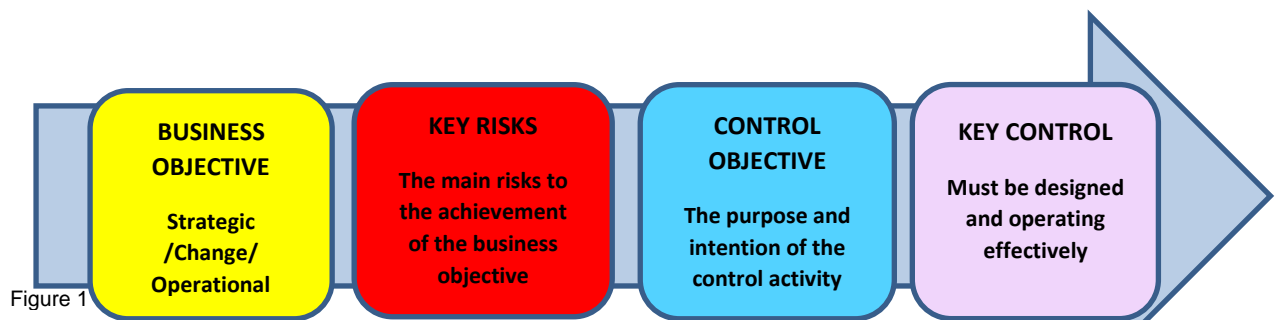
By integrating risk management with our key business planning and performance management processes, we can better identify emerging risks, manage and mitigate threats and exploit opportunities for change and growth. We must ensure that our risk vision, culture, appetite, governance and resources are aligned to the achievement of our objectives and support risk intelligent decision-making. To ensure an consistent and cohesive organisational approach we have developed a Risk Management Framework comprising a Risk Management Policy, Strategy, Appetite Statement, Process Guide and Risk Registers. Our approach will be further supported and enhanced through the use of performance and risk management software.

OUR RISK MANAGEMENT VISION

To be a risk intelligent Council; where risk management is fully integrated into our decision making and business processes, enabling the Council to deliver more cost efficient and effective services, be innovative and enterprising, to achieve best value and to continuously improve.

OUR RISK CULTURE

To be effective, process must follow culture. Changing our risk management processes and procedures will not create and deliver value to our organisation if our organisational culture remains static. Public sector bodies have traditionally had a culture of risk avoidance. In these changing and challenging times however, Perth & Kinross Council alongside our other public sector partners must become more risk intelligent in our approach to managing uncertainty, to enable us to exploit opportunities and maximise potential benefits as opposed to being solely focussed on minimising potential threats.

If we are to continue to be successful, we must recognise that risk-taking is not only inevitable but necessary.

The tone set at the top is crucial to successfully developing a risk intelligent environment. At a political and strategic level therefore, we advocate proactive risk management throughout the whole Council. In doing so we recognise and accept that we will not always get everything right as we strive to design more effective solutions which better meet the needs of our communities and that a "blame culture" will stifle change and innovation potentially hindering or derailing progress.

We want to create an authorising environment where our elected members and staff understand the value of risk management and are supported to make appropriate risk-based decisions and to take personal responsibility for the management of risk at every level. Key business risks will be monitored at the highest level but we will also be continuously reviewing the effectiveness of our risk management processes; responding positively to challenge and learning from mistakes.

Developing a more risk intelligent culture takes time and will require meaningful changes to be made to our established ways of operating.

What does a risk intelligent organisation look like?

A risk intelligent organisation does not seek to eliminate risk, or even to minimise it in all cases. Instead, it seeks to manage risk exposure across all parts of the organisation, so that, at any given time, it is incurring just enough of the right kind of risk to effectively pursue its goals and objectives.

A risk intelligent organisation:-

- understands that risk management must be integrated into core business processes
- assumes turbulence is inevitable and emphasises prevention and preparedness to improve organisational resilience and agility
- is vigilant for a broad range of opportunities and risks across the whole organisation
- acknowledges the need for specialist controls in some business areas, but where possible seeks to harmonise, synchronise and rationalise risk management and controls
- considers interactions among multiple risks as opposed to focussing on a single risk or event, and considers the combined impact
- creates a common risk language within the organisation so that there is a consistent method and approach to identify, assess, plan, implement, monitor and manage risk across the whole Council
- encourages informed risk taking for value creation and opportunities, rather than focussing on pure risk avoidance

We will support the Council to be risk intelligent by ensuring that:-

- everyone understands the Council's approach to risk; its values, appetite and processes
- elected members and staff have the necessary knowledge and tools to enable them to make risk-based decisions and manage risks appropriately and effectively in their day to day activities
- we adopt and apply our risk management approach consistently across all business activities of the Council from strategic planning to day-to-day operational service delivery
- within the Council we are all comfortable acknowledging and talking openly about risk and that we develop a common risk vocabulary that promotes shared understanding
- we all understand and promote the value that effective risk management can bring to the organisation
- we all take personal responsibility and recognise when we need to involve others
- we create a safe environment for individuals to constructively challenge others in respect of risk, including those in authority, without fear and retribution and we respond positively
- we are a learning Council, continuously seeking to improve our collective understanding of risk management, learning from our mistakes

OUR RISK CONTEXT

Perth & Kinross Council is a complex business, delivering a broad range of services to the community. As a public body it is highly regulated and accountable for its performance to a wide range of stakeholders and the community.

Despite significant financial constraints and a rapidly changing public sector landscape, the Council is under pressure not only to sustain current service delivery, but to meet ever increasing demand pressures, improve our performance and deliver best value for our community. To simply remain sustainable we need to take a more entrepreneurial approach to how we do business. We must seek out and develop new and innovative ways to deliver services, designing solutions through partnerships and increased collaboration with the public, private and third sectors and with communities themselves. With enterprise, innovation and collaboration however, comes additional uncertainty which will create a new and very different risk landscape for public authorities. The need for effective risk management within the Council therefore, has never been more crucial.

This Risk Management Strategy sets out the Council's approach to risk management. It does not identify what our risks are, or state how these should be managed, as risk management should be a fluid and iterative process. Instead, it sets the tone and direction for the organisation and provides the blueprint for how our risk management vision and objectives can be realised.

Our approach to risk management will be determined by our own risk environment; it is important that we understand our local context and the internal and external factors that shape or influence our risk environment.

> - Internal factors include our culture, standards and values, our resources and capabilities, our governance arrangements, our internal stakeholders, contract, commissioning and partnership arrangements, our strategic aims and objectives.

> - External factors include decreasing budgets, a rapidly changing policy environment, increasing pressure on public services, an ambitious national public sector reform agenda, challenging national targets and outcomes and a legislative drive towards empowering communities to have more influence and control on decision making and the delivery of local public services.

These factors need to be known, understood and evaluated before we can manage risk effectively within the organisation.

OUR RISK APPETITE

Knowing and understanding our risk appetite will improve the effectiveness of our risk management process. Risk appetite is the amount of risk that an organisation is willing to accept in pursuit of its objectives. Organisations will have different risk appetites depending on their sector and risk culture and, even within each organisation, a range of appetites exist for different risks which may change over time. As risk is such a dynamic thing, it is impossible to make a definitive appetite statement. The impact of uncertainty can vary widely depending upon specific circumstances at any given time.

Our Risk Appetite Statement provides stakeholders with a high level understanding of the parameters within which Perth & Kinross Council will tolerate certain key business risks. It is

designed to guide and support elected members and staff to make better risk based decisions in their day to day activities; to enable the Council to achieve its goals and support sustainability. As our approach to risk management matures we will be able to further develop and refine our organisational risk appetite to reflect and respond to the current operating environment.

OUR APPROACH

Risk management standard

The approach is based on best practice industry standards including the International Standard in Risk Management – ISO: 31000, the Office of Governance & Commerce (OGC) and the Management of Risk (M_o_R®) Guidance.

Risk categories

Local Government is a complex business, presenting a wide and diverse range of opportunities and threats to the achievement of our objectives. Our approach categorises risks which the Council must manage as:

1. **Strategic:** risks which potentially impact upon the Council's ability to achieve its corporate objectives

2. **Change:** those risks related to change management or investment programmes or specific projects

3. **Operational:** risks which impact upon the Council's ability to deliver its services to the public and / or its support functions

Risk factors

Whilst we have three broad categories of risk to consider, the factors which impact upon these are wide ranging and diverse. Threats and opportunities to our strategic, change and operational objectives can emerge from a number of areas; both from the internal environment and the external environment. Similarly, the consequential risks can impact a number of areas. More information as to the factors which may impact upon our risk profile are set out in the Risk Management Process Guide.
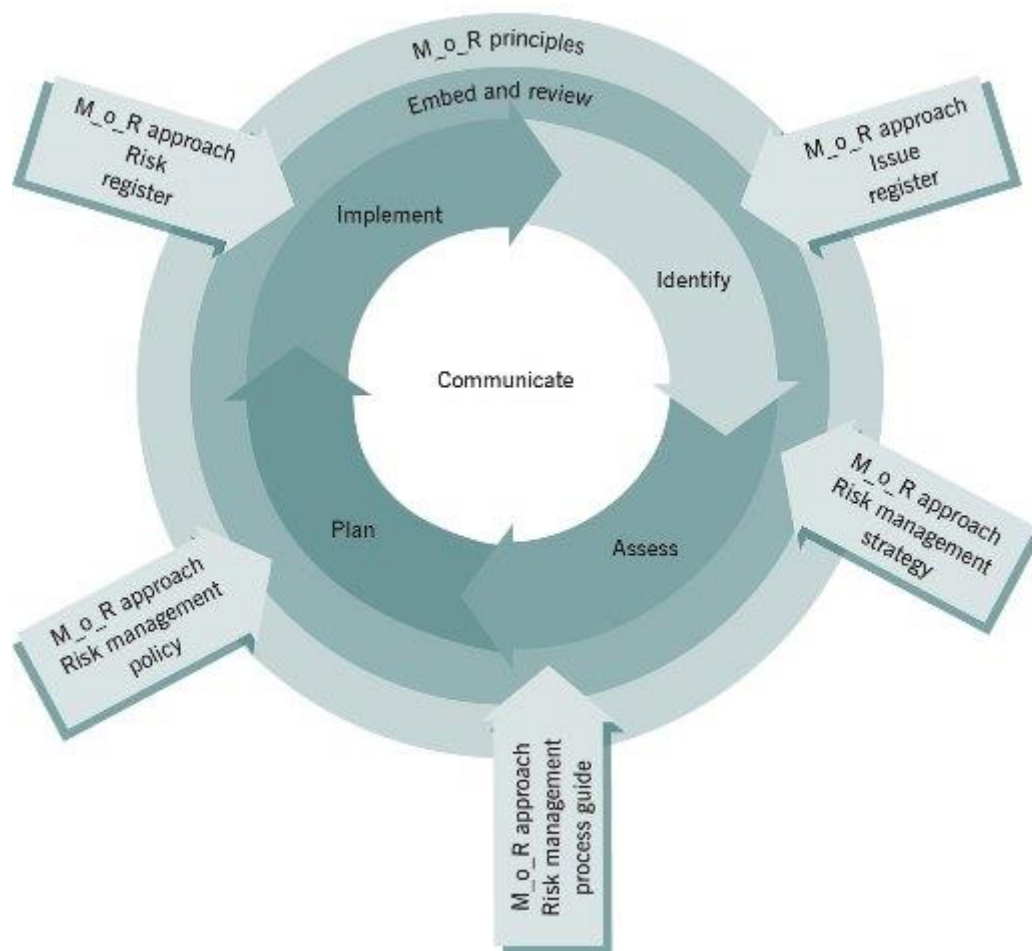
Risk Management Process

The Risk Management Process is a core component of the Risk Management Framework. It provides a structured approach to the identification, evaluation and management of risk at every level within the organisation. It enables the Council to prioritise risks in a consistent manner based on an impact/probability matrix analysis. By taking an integrated, organisation wide approach to the management of risk, the Council will be better placed to realise potential benefits and achieve greater value from the risk management process as a key driver in service performance and improvement.

There are four steps in the Risk Management Process

1. Identification
2. Assessment
3. Planning
4. Implementation and Monitoring

Each of the steps is described in detail in the Risk Management Process Guide.

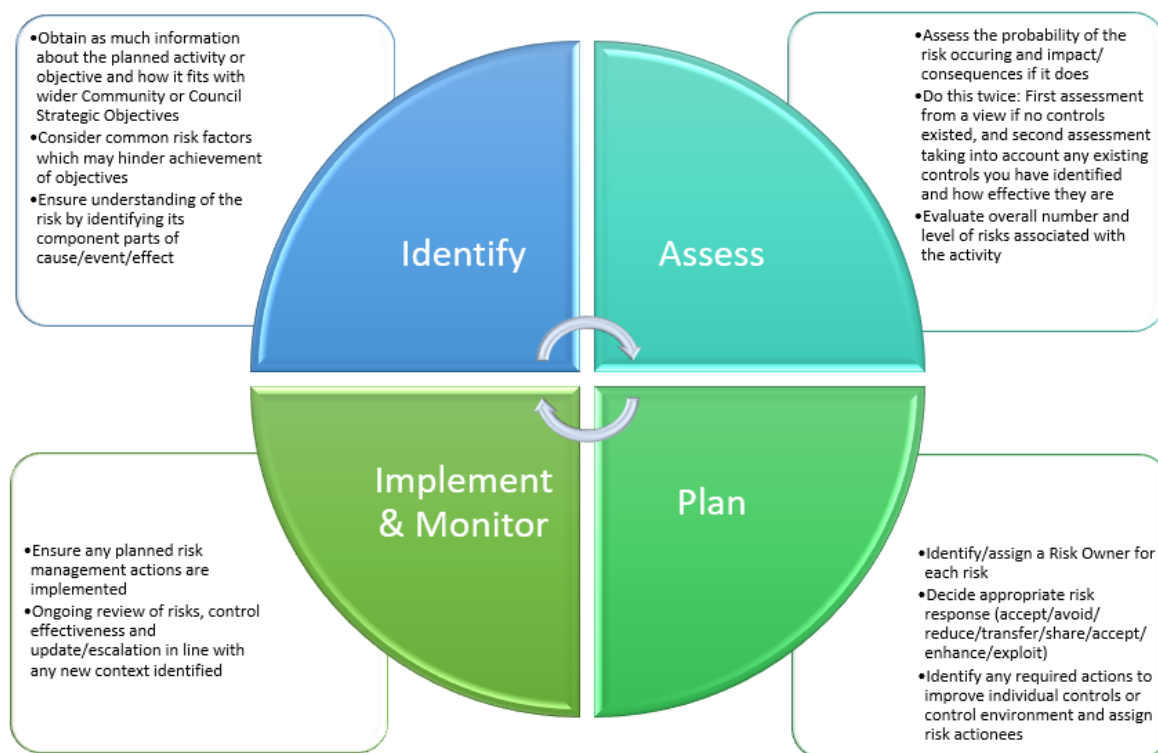The Risk Management Process as a whole is illustrated at Figure 2 below

Figure 2

If the Council is to derive real value from its risk management process then it must be a fluid and ongoing process, implemented by people at every level of the organisation. It is important that we have sight of our risks both vertically and horizontally across the organisation as a whole. This organisation wide approach to risk management ensures that our risk resources and capabilities can be deployed to maximum effect and are aligned to the Council's strategic aims.

The Risk Management Framework should be used proactively to identify threats and opportunities to the achievement of our corporate and community objectives. It should be an intrinsic part of our business planning and performance management processes at strategic, operational and interagency level. Risk management is dynamic therefore it cannot be a six monthly or annual stand-alone process for the purposes of reporting; it must be embedded into our day-to-day business activities.

The purpose of Risk Management is to eliminate the barriers to our success. If risk management is to be a true enabler of improved organisational performance, it is vital that individuals recognise that risk management is a means to that end – and the process is not an end in itself.

OUR RISK GOVERNANCE STRUCTURES

While it is important to ensure that the Council is '*doing risk management right'*, it is equally important to '*do the right risk management'*. This includes having processes in place so that the appropriate levels of management have oversight of the different levels of risk across the

department. The risk hierarchy defines accountability to identify, assess, plan, implement, monitor and manage risk throughout the organisation.

It is vital that risk is managed effectively at every level of the organisation. This means that risk must be fully integrated into our business processes and systems to ensure that risk is being identified, managed and reported at each level. Accountability for risk will depend upon the nature of the risks.

The Council's integrated business planning system cascades from the Corporate Plan and Local Outcomes Improvement Plan through to Service and programme plans and strategies, operational team and project plans, and then distilled into individual performance and development plans. The planning cycles provides an opportunity for the Executive Leadership Team (ELT), the Strategic Leadership Team (SLT) and Strategic Lead Management Teams to undertake analysis regarding emerging or known risks that may impact on their purpose and objectives.

Roles & Responsibilities

- The Council agrees the Risk Management Framework comprising the Risk Management Policy, Strategy, Process Guide, Registers and Risk Appetite Statement for the organisation and, together with the ELT it champions the risk management principles, establishes the risk appetite and sets the tone for how risk will be managed across the whole organisation.

- The Chief Executive has overarching responsibility for ensuring adherence to the Risk Management Policy within the organisation and as such shall ensure that the Council's Risk Management Framework is regularly monitored and reviewed to ensure its continuing effectiveness in managing risk and delivering value.

- The ELT is responsible for implementing the Risk Management Framework at strategic level, reviewing risk evaluation against organisational risk appetite and ensuring that risk management is integrated into the Council's business processes and practices.

- The Strategic Leadership Team (SLT) manage and monitor strategic risks and those operational risks which have a cross-service impact or potentially impact upon the delivery of strategic objectives. The SLT ensures that the Risk Management Framework is implemented and integrated into operational business practice across the organisation. They ensure that risks have an appropriately named owner, resourced action plan and named actionee(s).

- Strategic Leads and their Management Teams implement the Risk Management Framework and integrate effective risk management into their own business processes and practices. They ensure that risks are identified against the delivery of strategic and operational objectives and are the key lever for the escalation of risks to the SLT if they can no longer be effectively managed within the service or present a wider organisational or strategic risk. They identify risk owners and actionee(s) as appropriate and put in place a resourced action plan in respect of identified risks.

- Programme and Project Boards manage all risks associated with the delivery of change programmes or specific projects. They ensure that risks have an

appropriately named owner, resourced action plan and named actionee(s). Ensure that Priority 1 & 2 risks are escalated to:-

> ➢ The Transformation Board so that it can be considered if they have an impact which will impact upon delivery of the programme/project and if any mitigation action is required.

> the SLT if they have an impact upon the delivery of a strategic objective or if they have the potential to impact upon the operational objectives of more than one service; or
> ➢ the Strategic Lead Management Teams if they will impact upon operational targets or objectives for that Service.

- Operational teams are responsible for ensuring that the risk management framework is implemented at operational level. They manage the day to day risks associated with delivery of the service or support function and provide reasonable assurance to Senior Management Teams that the main tactical and operational risks arising from service operations are being managed.

- The Council's Risk Guidance Network comprises risk practitioners who provide technical advice, guidance and support to the organisation and work with services to ensure that the management of risk is integrated with key business process in terms of planning and performance.

- The Council's Policy & Governance Group (a sub-group of the SLT and chaired by the Strategic Lead for Legal & Governance Services) develops, leads on and co-ordinates the Council's risk management approach, including the periodic review of Council's Risk Management Framework and any ancillary documents. It provides leadership to ensure that a consistent approach is adopted and implemented throughout the organisation and that appropriate governance and controls are in place.

- Internal Audit provides an annual audit of the Council's risk management process and an independent objective opinion on its operation and effectiveness as part of the review of corporate governance arrangements.

- The Audit and Risk Committee oversee, monitor and review the strategic arrangements for the assessment and management of risk and the Council's system of internal control.

- The Finance and Resources Committee determines the Council's policies and strategies in relation to risk management.

OUR RISK ASSURANCE FRAMEWORK

Risk management is an integral part of the Council's internal control system and the broader corporate governance framework however, we must also be able to provide assurance as to the effectiveness of our risk management process to external stakeholders.

The different levels of responsibility and accountability within the risk assurance framework, together with our risk management principles and approach can be thought of as "lines of

defence" in terms of mitigating and managing risks and protecting the Council from the impact of those risks if realised.

> **The first line of defence in** any organisation is the risk culture. The tone that we set at the top will be the foundation for good risk management. We must all communicate our risk approach and values consistently across the Council at every level and reinforce this by our actions and behaviours.

> **The second line of defence** are the divisional management teams/ programme boards/ projects teams who own the risks and are responsible and accountable for the identification and management of the risks within their areas.

> **The third line of defence** are those with oversight responsibility – this will be the Strategic Lead Management Teams/SLT/Transformation Board/ ELT depending upon the nature and level of the particular risks.

> **The fourth line of defence** comes from the Council's corporate control and compliance functions such as Finance, Legal, HR, Corporate Risk, Procurement, Information Technology, Information Security & Compliance, and Health & Safety. These functions must collaborate with process owners to develop and monitor controls to mitigate identified risks. They also play a key role in independently evaluating risk and alerting management to emerging risks.

> **The fifth line of defence** are our internal and external audit functions which review controls and management procedures, identify issues and improvement opportunities and evaluate the overall design and effectiveness of the Council's internal control processes.

> **The final line of defence** is the Council's Audit and Risk and Finance and Resources Committees. The Audit and Risk Committee oversees the Council's risk management activities and the effectiveness of the internal controls. The Scrutiny and Performance Committee ensures that the risk management framework is aligned to the Council's objectives and supports continuous improvement in risk performance.

OUR COMMITMENT TO CONTINUOUS IMPROVEMENT

We are looking for our risk maturity to develop and grow. We recognise the importance of learning from mistakes and ensuring that our risk management framework remains vital and dynamic to meet the challenges of 21st Century local government.

We will regularly monitor and review our Risk Management Framework to ensure that:

- it remains relevant and fit for purpose as our internal and external context changes
- it is effective in mitigating threats and maximising benefits to our organisation and the community
- our risk criteria remain relevant in a rapidly changing public sector landscape
- as an organisation we can capture learning from our risk management activities
- we are achieving our expected risk management outcomes

The Risk Management Process provides more detailed guidance on how we manage risk.