Comhairle Contae Chorcaí
Cork County Council

Risk Management

Risk Management Policy

Cork County Council
Risk Management Policy

Scope and Rationale

Cork County Council is committed to the management of risk as an integral part of its operations, implementing strategies to minimise threats to the achievement of organisational goals and service delivery objectives.

Effective risk management will allow us to:

- Make informed decisions
- Manage risks at tolerable levels
- Strengthen our governance procedures

Risk Criteria

The strategic objectives from the Corporate Plan inform operational objectives in the Annual Service Delivery Plan.

A risk is a threat to the achievement of the Council's service delivery objectives.

A risk is 'the effect of uncertainty on objectives' (ISO Standard 31000:2009 Risk Management).

The risk criteria are the terms of reference against which the significance of a risk is evaluated. (ISO guide 73)
The "Consequences" element describe the loss or damage that would occur should an objective not be met. This loss may be of Financial, Compliance or Reputational nature.

Risk Appetite is the amount and type of risk that an organization is prepared to pursue, retain or take. It will be set and reviewed by the Chief Executive in consultation with SMT. Conflicting interests, for example where a business decision may exceed stated risk appetite levels, will be dealt with at SMT.

In terms of Risk Appetite, the Council, Chief Executive, and management team encourage:

- Taking of controlled risks,
- Grasping of new opportunities
- Innovative approaches to achieve objectives.

However, all resultant risk exposures should rest within agreed risk appetite limits and should not prejudice the following:

- Reputation or relationship with other state bodies and agencies
- Organisational performance and particularly operational efficiency and effectiveness
- Control environment and internal control systems
- Adherence to governance, legal and regulatory obligations.

Objectives of this Risk Management Policy:

- Provide a robust risk management structure operating an effective system of risk identification, analysis, evaluation and treatment within all areas and all levels of the organisation.
- Make the management of risk and risk management ethos as an integral part of our business processes.
- Avoid exposure to significant reputational or financial loss.
- Contribute to the achievement of the organisation objectives at enterprise level and operational level.
- Set out the roles and responsibilities for Risk Management within the organisation.

Roles and responsibilities

The Chief Executive is responsible for establishing and maintaining a sound system of internal Risk

Management control that supports the achievement of policies, aims and objectives. This system should be able to evaluate the nature and extent of these risks and manage these effectively.

The Corporate Development Management Group is responsible for the approval of the Risk Management policy, monitoring of its effectiveness and for the development and approval of an enterprise Risk Register.

The Chief Risk Officer role has been assigned to the Director of Corporate Services by the Chief Executive. The Chief Risk Officer oversees policy development and Risk Management implementation across Cork County Council. The Chief Risk Officer is responsible for the development and provision of risk management awareness training as well as specific training and education programmes throughout the organisation. This training and education are to address the needs of all directors, employees and contractors including senior management.

The Director of Services/Head of Function/ Divisional Manager

Ensure compliance with risk management policy.

Identify key risks and related issues and prepare/review the Risk Register for their directorate.

Propose new risks to CDMG for inclusion in the Enterprise Risk Register where considered relevant.

Ensure ~~p~~procedures for managing risk are fully understood and implemented by all staff.

Provide periodic reports to the Risk Oversight Committee on Risk Management practice and outcomes.

Identify shared risks and interdependencies and record them accordingly in the risk register.

Anticipate and respond to changing social, environmental, legislative, political, economic, technological, competitive, and customer requirements.

Promote a culture of preventing injury, damage and losses and reduce the cost of risk.

Raise awareness of the need for Risk Management across all activities.

Ensure that the necessary resources are made available to those accountable and responsible for the management of risk.

The Risk Liaison is appointed in each Directorate and responsible for maintaining the risk register for the directorate.

The Portfolio owner- The Director of Services/ Head of Function is the Portfolio Owner of their directorate's risk register.

The Risk Owner is the member of staff responsible for the specific risk listed in the risk register.

The Task owner is the member of staff responsible for the specific task relating to a specific risk in the risk register.

All employees are responsible for managing risk in so far as is reasonably practicable within their area of

activity. All members of staff in the Council have a part to play in managing risk by being aware of the nature of risks in their day-to-day work, monitoring the effectiveness of management procedures created to mitigate those risks identified and responding to the changing nature of the risks faced by the organisation.

The Risk Oversight Committee's key role is to oversee and monitor Risk Management Policy and ensuring that Corporate and Directorate risk registers and related management actions are established throughout Cork County Council. Terms of reference document in Appendix 2.

The Safety Management and Monitoring Committee (SMMC) monitors compliance with our safety management system and will inform the Risk Oversight Committee of any new permanent or temporary risks which it feels should be reviewed by the ROC for inclusion in the risk register. It is accepted good practice to provide a forum for identifying and aligning the safety risks with the corporate risk register.

The Audit Committee's role is to review the appropriateness and implementation of Risk Management arrangements. The review may include an internal audit on the appropriateness and efficacy of the risk management policy and processes.

Risk Register – Measuring Risk Management Performance

The enterprise risk register as well as all risk registers of individual directorates are stored and managed in CalQRisk, the software platform chosen by Cork County Council for risk management and reporting.

Risks with a residual risk value of <5 and consequence rating <5 are not on the risk register.

A review of the Risk Register should be on the agenda of each directorate's SMT meeting.

Appendix 1 Risk Register Template
Appendix 2 Risk Criteria
Appendix 3 Risk Management Process
Appendix 4 ROC Terms of Reference

Other references:
ISO guidance 31000:2018
DPER RM Guidance

Last reviewed on: 25th January 2024
Next review due: January 2027

Appendix 1 – Risk Register Template

Risk Register

Cork County Council

Seq	Risk ID	Category	Risk Description	Portfolio Owner	Risk Owner	L	C	R	Controls	L	C	R	Additional Mitigation Options	Theme	Corporate Plan	Actor - Tasks	Linked Risks
1	56673	Technology - Technology	Successful Cyber Security attack and/or unauthorised access - Cyber attack could result in Service disruption, complete loss of IT systems, Data loss, Data breach Source: New threat, attack, or vulnerability Consequences: Information Security GDPR breach	Patricia Liddy	Jacqueline Hunt	5	5	25	Working through Implementation of CIS controls and implementation of PS Cyber Security Baseline Standards ITIL Availability and Capacity Management processes All security incidents and new threats managed effectively Number of patches installed Number of security threats responded to Number of staff security	5	5	25	Security Monitoring - Manage SOC Functions CIS Benchmarking and implementation Additional Security layers Security Awareness Email Phishing/DMARC Solution McAfee Upgrade Windows Login MFA Phishing - Restricted Access Group	7-Governance and Democracy	7.2 Governance		76600 - Service Disruption (Cyber Attack)
2	56659	Legal & Regulatory - Regulation	Inadequate Integrated Enterprise Resource (ERP) Systems - Source: Consequences: See Evaluation comments below	Patricia Liddy	Loraine Lynch	5	5	25	A dedicated team has been set up to review and put in place the plan to identify, implement and deliver a new system	5	4	20	Resource a dedicated Systems Project Team in Finance Source external expertise to develop a strategy Draw up implement plan	7-Governance and Democracy	7.4 Business, Service & systems		83885 - Failure of a key system (Integra (FMS))
3	56663	Economic - Economic	Funding Uncertainty arising from ext. and int. sources Inequitable distribution of National funding - Local Government Fund Property Tax Receipts Source: Irish Water Payments Grants Haulbowline Project funding Boundary transfer funding/compensation	Patricia Liddy	Loraine Lynch	5	5	25	Irish Water/LA Sectoral Group Meetings Budget Control Local Property Tax Ongoing DECLG contact Ongoing IOG engagement AIRO Report submitted to Government	4	4	16	Provide Visibility of future Capital Demands/identify and Prioritise review areas/Development of reporting processes (integra is not a competent budget management tool).	5-Capacity for Growth	5.8 Projects of Scale		

Appendix 2 – Risk Criteria

Risk Criteria

Criteria	5 Substantial	4 Significant	3 Moderate	2 Minor	1 Negligible
Safety	Incident leading to death or major permanent incapacity. Permanent psychosocial functioning incapacity.	Major injuries/long term incapacity or disability (loss of limb) requiring medical treatment and/or counselling. Impaired psychosocial functioning >6 months	Significant injury requiring medical treatment e.g. Fracture and/or counselling. Reportable to the HSA or Gardai. >3days absence. 3-8 days extended hospital stay. Impaired psychosocial functioning for 1 to 6 months.	Minor injury or illness requiring first aid treatment. <3 days absence. <3 days extended hospital stay. Impaired psychosocial functioning between 3-30 days	Adverse event leading to minor injury but not requiring first aid. No impaired Psychosocial functioning
Service	Totally unsatisfactory service user outcome perhaps resulting in Departmental inquiry, Garda investigation or likely to result in High Court procedures.	Unsatisfactory service user experience resulting in threats of legal action at Circuit Court level or brought up at Council Chamber.	Unsatisfactory service user experience possibly resulting in minor financial or entitlement loss. Likely to involve retrospective action from senior line management.	Unsatisfactory service user experience related to poor treatment/ waiting times/ inadequate information. Likely to involve supervisor input.	Minor impact on service user experience i.e. due to inadequate information provision. Quickly rectified by front line staff.
Approvals / Compliance	Gross failure to meet external standards/legislation resulting in external body investigation or media exposure. Major reputational or financial implications.	Repeated failure to meet external standards or legislation. Likely to require investment/retraining/significant process change on foot of a formal report or external	Repeated failure to meet internal standards likely requiring an appropriate management action plan.	Single failure to meet internal standards. Local Management can easily address same after minor investigation.	Minor non compliance with internal standards. Small number of minor issues requiring improvement.
Reputation	Major adverse publicity circulated in national media for >3days. Comments by Minister/Taoiseach or questions in Dail. Very significant reduction in public confidence. Calls for sanction of individual officials. Public Inquiry.	Very significant adverse publicity circulated in National media for a period less than three days. Chief Executives or Mayors asked to formally comment. Specific written inquiries from Department. Performance brought up in Council Chamber	Significant adverse publicity circulated by Local media. Local demands for action. Likely to require a comprehensive review and active engagement with media. Informal inquires from Department.	Some local media coverage and public concern. May require internal investigation.	Rumours but with no media coverage or voiced public concerns. No specific action needed.
Financial	>100k	20-100k	5-20k	<1k - 1.5k	<1k

LIKELIHOOD				
5 Very High	4 High	3 Medium	2 Low	1 Very Low
Once per Quarter, or more frequent	Once per Year, or more often	Once in 3 years	Once in 10 years	Once in 30 years, or less often

Risk Management Process

Introduction

"The board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems." (UK and Irish Corporate Governance Code 2012)

This document describes the main aspects of the risk management process employed in Cork County Council and which is supported by the use of the CalQRisk risk management information system.

CalQRisk has an embedded database of the significant risks that organisations are exposed to, including their associated controls. This allows us to conduct a top-down assessment into all key areas of risk while allowing us to add specific risks that we identify and are particular to the organisation.

Definitions

The language used in the description of our risk management process is consistent with that in the ISO 31000:2018 risk management standard. A list of the key terms and their definitions is shown below.

risk	effect of uncertainty on [the achievement of] objectives
risk management	coordinated activities to direct and control an organisation with regard to risk
risk criteria	terms of reference against which the significance of a risk is evaluated.
risk appetite	amount and type of risk that an organisation is willing to pursue or retain.
risk capacity	is the maximum amount of risk which the organisation is technically able to assume before breaching one or more of its capital base, liquidity, borrowing capacity, reputational and regulatory constraints.
risk assessment	overall process of risk identification, risk analysis and risk evaluation
risk identification	process of finding, recognizing and describing risks
risk owner	person or entity with the accountability and authority to manage a risk
risk analysis	process to comprehend the nature of risk and to determine the level of risk
risk evaluation	process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable
likelihood	chance of something happening
consequence	outcome of an event affecting objectives
level of risk	magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood.

risk treatment	process to modify risk
control	measure that is modifying risk
inherent risk	risk posed before the systems and controls are considered.
residual risk	risk remaining after risk treatment /controls are considered.
risk register	record of information about identified risks

The Process

The Risk Management Process employed by CalQRisk Co follows the guidance in ISO31000; the key steps are outlined in Fig 1 below.

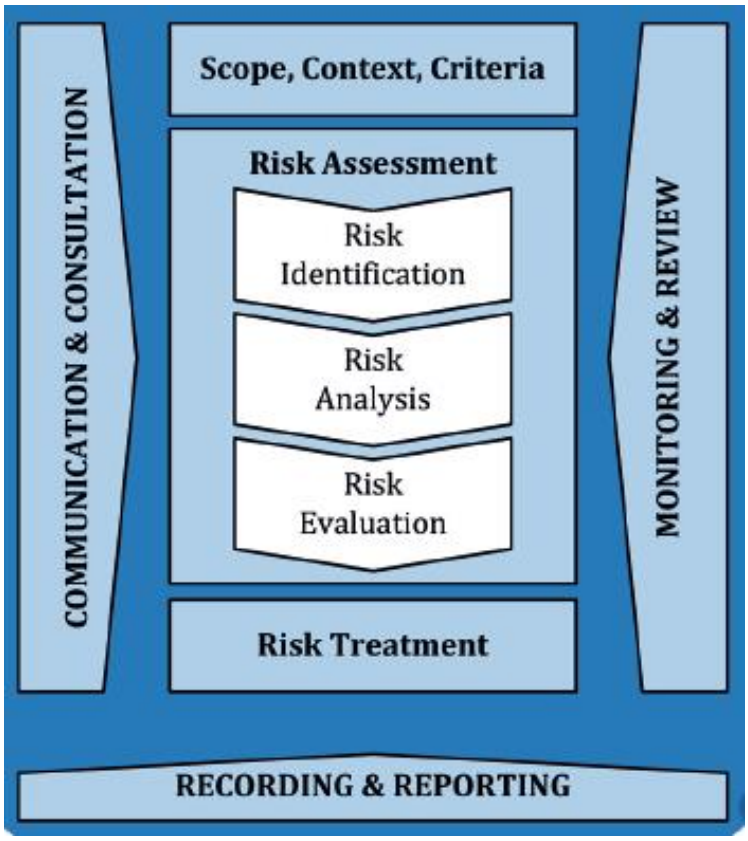

Fig 1. The Risk Management Process

The process comprises five core steps that although shown sequentially, in practice occur in an iterative way. These steps allow risk to be identified and understood, evaluated against the risk criteria, and be treated if necessary.

When Applied

The Risk Management process is applied:

- initially, to seek assurance that all material risks have been identified and are being managed within acceptable limits.
- when objectives are set or changed.
- when there are changes to the internal / external environment.
- to support compliance with regulations or contracts.

Establishing the Context

The first step in applying the risk management process is to establish the context in which the risk management is carried out. This has been completed for Cork County Council and details can be found in the Risk Management Policy.

The context broadly describes:

- the objectives of the organisation
- the internal and external environment
- the Risk Criteria used to evaluate the significance of risks
- the Risk Appetite as defined / approved by the Senior Management Team.
- the stakeholders that have an interest in the risks affecting the organisation
- the scope of the risk assessment; what areas will be covered. (Risk Assessment Framework)
- the Key Risk Indicators (KRIs) that reflect trends in how risks are impacting the organisation

Risk Criteria

The terms of reference against which the significance of each risk is evaluated were defined in a workshop session in which risk liaisons attended. Full details of the agreed criteria are in Appendix 2.

Risk Assessment

Risk assessment comprises three steps: **risk identification, risk analysis and risk evaluation**. The risk framework (See Fig.2) is used in the identification phase to bring focus on the key areas that represent sources of risk that threaten the achievement of our objectives. The framework includes “Compliance risks”; that is, those risks that arise due to absence or failure of required controls as well as operational risks that threaten the financial and operational goals of the organization. Using CalQRisk, selecting the key areas (Categories and sub-categories), the key known risks are presented and analysed using sets of detailed questioning that checks for the existence of controls, their adequacy and effectiveness. Once analysed the risks are evaluated against the defined Risk Criteria to determine if they can be accepted / tolerated or whether they need to be treated, that is, whether more can /should be done to make the risk acceptable. In some instances, the decision may be to terminate or avoid the risk, that is, to cease doing whatever activity gives rise to the risk.

Fig 2. The Risk Framework

When assessing and estimating risk, consideration is first given to **the inherent level of risk**. (Pre-Controls) This represents the risk posed before the systems and controls which relate to the risk are considered. **Residual risk** (Post-Controls) represents the level of risk after consideration of the adequacy and effectiveness of policies, processes, procedures, systems, training, and other controls that the company has put in place to manage and mitigate the risk. The product of Likelihood and Consequence provides the organisation with a risk rating, which indicates the magnitude of a risk. The residual risk is calculated in a consistent manner by the software application – CalQRisk - that we use to assess and manage the risks in the company.

It is a known challenge to define precisely what the inherent level of risk is. The approach we have taken is to consider what the level of consequences might be if several key controls failed / were not in place, and how likely / how soon might the consequences arise. In order to estimate the residual risk, each question that is posed regarding the risk is individually weighted and can reduce either or both the likelihood or consequences of a risk. When all questions have been answered the system (CalQRisk) calculates the residual risk.

Risk Evaluation

When a risk has been thoroughly analysed and the residual risk is known, this is compared with the risk criteria and if it is within what is considered the acceptable range (risk appetite) then the evaluation decision would be to “Tolerate” or accept the risk. If the level of risk is outside the risk appetite and it is felt that additional mitigation could bring the risk within the appetite, the evaluation decision would be to “Treat” the risk. In other cases, where the risk is outside the appetite the decision might be to “Terminate” or avoid the risk altogether. Some risks that are nominally outside the risk appetite, and where no additional mitigation options have been identified, may be tolerated / accepted if it is considered that it is part of doing business. In these cases, the risks will be constantly monitored for opportunities to mitigate further.

Risk Register

At any point during the assessment process a risk register can be generated which ranks the risks in order of magnitude (Level of Residual Risk). The register includes all risks that have been analysed and / or evaluated. Details in the risk register include:

- Unique risk ID number
- Category to which the risk belongs
- Description of the risk
- Risk Owner (person primarily responsible for managing the risk)
- Pre-Controls (Inherent) level of risk (Likelihood, Consequence and Rating)
- Mitigating controls in place
- Post-Controls (Residual) level of risk (Likelihood, Consequence and Rating)
- Additional mitigation options for consideration.

The residual level of risk is calculated by the risk information management system we use (CalQRisk) and this includes consideration of the adequacy and effectiveness of the controls.

The risk register is a key report used in communicating the risk profile to stakeholders; this is presented to SMT on a regular basis.

Risk Treatment

When risks have been fully assessed, those that have been classed for treatment are reviewed and where mitigation actions are identified these are assigned as “Tasks” to individuals for completion within a certain time period.

We use the built-in “Action Manager” in CalQRisk to assign and manage these tasks. When a task is assigned the system automatically sends the task owner a notification that they have been assigned a task and when it must be completed by.

When a task is completed, the risk is re-assessed; this might be simply changing a “No” in the question set to a “Yes” and letting the system re-calculate the residual risk. In the case of user added risks the Risk Owner can manually adjust the residual level.