Dublin Docklands Development Authority

2.4 Integrated Risk Management

April 2012

2.4 Integrated Risk Management

Index

Annexes

Note:

This policy is being developed in conjunction with MAZARS (our Internal Auditors) so as to create a common starting point for the Authority and Audits to develop a risk framework for both purposes.

1 Introduction

"An effective risk management system identifies and assesses risk, decides on appropriate responses and then provides assurance that the chosen responses are effective"

Code of practice for the Governance of State Bodies 2009 [1]

The importance of Risk Management has been emphasised in publications such as the Mullarkey Report, the Department of Finance Guidelines on Risk Management and most recently the Code of Practice for the Governance of State Bodies. The latter two documents in particular contain guidance on the objectives, structures, processes and tools that should be used to effectively manage organisational risks. These documents are also supplemented by a wealth of best practice publications which have emerged in recent years.

This document describes the risk management framework in operation within the Dublin Docklands Development Authority. The framework is designed to support the ongoing monitoring, review and management of risks and was developed with reference to the Code of Practice for the Governance of State Bodies 2009 and other published guidance for risk management in the public and private sector.

2 Risk Management in the Dublin Docklands Development Authority

In 2010 the Dublin Docklands Development Authority implemented an enhanced formal Risk Management Framework within the organisation.

2.1 Risk Management Objectives

The Authority is committed to establishing and maintaining a robust risk management framework that supports the ongoing management of risk in accordance with the established risk appetite and corporate strategy.

The objective of this policy is to ensure the Authority is equipped to monitor and manage its key risks in line with best practice. Specifically, this framework has been developed to ensure:

I. The risk framework addresses the requirements of the Code of Practice for the Governance of State Bodies (2009)

II. That a practical process for the formal management of organisational risks is established and that the process is maintained on an ongoing basis

3 Risk Appetite

The Code of practice for the Governance of State Bodies 2009 establishes a requirement for the Executive Board of the Dublin Docklands Development Authority to establish the organisation's

[1] *Derived from UK Independent Commission on Good Governance in Public Service.*

risk appetite. Risk appetite can be defined as *"the amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time*[2]*"*.

DUBLIN DOCKLANDS DEVELOPMENT AUTHORITY RISK APPETITE STATEMENT

The Authority is not willing to accept risks in most circumstances that may result in reputation damage, financial loss or exposure, major breakdown in information systems or information integrity. As such it does not have a high risk appetite in relation to any areas of activity.

The Authority recognises that to successfully deliver on its mission, *"to develop the Dublin Docklands into a world-class city quarter paragon of sustainable inner city regeneration - one in which the whole community enjoys the highest standards of access to education, employment, housing and social amenity and which delivers a major contribution to the social and economic prosperity of Dublin and the whole of Ireland"*, the organisation must accept, tolerate and be exposed to a certain level of risk. Risk is inherent in every activity that the Authority is responsible for performing (from taking strategic decisions, to implementing supporting actions).

The Authority commits to utilising its defined risk framework as a tool to provide transparency on the risks inherent in organisational activities and to inform the Authority about potential or actual deviations from risk appetite. The management of risk within the risk appetite of Authority is supported by the wider risk framework set out in its risk management policy.

In addition to this general statement on risk appetite the Dublin Docklands Development Authority has also formulated a number of more detailed risk appetite statements by risk category.

The Authority will periodically (at least annually) review its risk appetite in light of changing circumstances in its wider environment, its organisational capacity to bear risk and the potential rewards associated with taking on an additional level of additional risk.

In deciding upon an appropriate risk appetite, a range of alternatives were considered, from high risk appetite to zero risk appetite, as presented in the following table.

Assessment	Description
High Risk Appetite	The organisation accepts opportunities that have an inherent high risk that may result in reputation damage, financial loss or exposure, major breakdown in information system or information integrity.
Medium Risk Appetite	The organisation is willing to accept some risks in certain circumstances that may result in reputation damage, financial loss or exposure, major breakdown in information system or information integrity.

[2] The Orange Book: Management of Risk – Principles and Concepts

Assessment	Description
Low Risk Appetite	The organisation is not willing to accept risks in most circumstances that may result in reputation damage, financial loss or exposure, major breakdown in information system or information integrity.
Zero Risk Appetite	The organisation is not willing to accept risks under any circumstances that may result in reputation damage, financial loss or exposure, major breakdown in information system or information integrity.

In recognition that risk may arise at multiple levels (from taking strategic decisions, to implementing supporting actions) and take many forms, the Authority has formulated a number of more detailed guiding risk appetite statements (see table below) to guide its staff in their actions and support their ability to accept and/or manage risks. The detailed risk appetite statements should also assist the Executive Board and management to monitor deviations from risk appetite on an ongoing basis.

Guiding risk appetite statements by risk category: the Authority has set a number of guiding risk appetite statements across the risk categories used within the risk register. For definitions of the risk categories please see Annex 2 to this document:

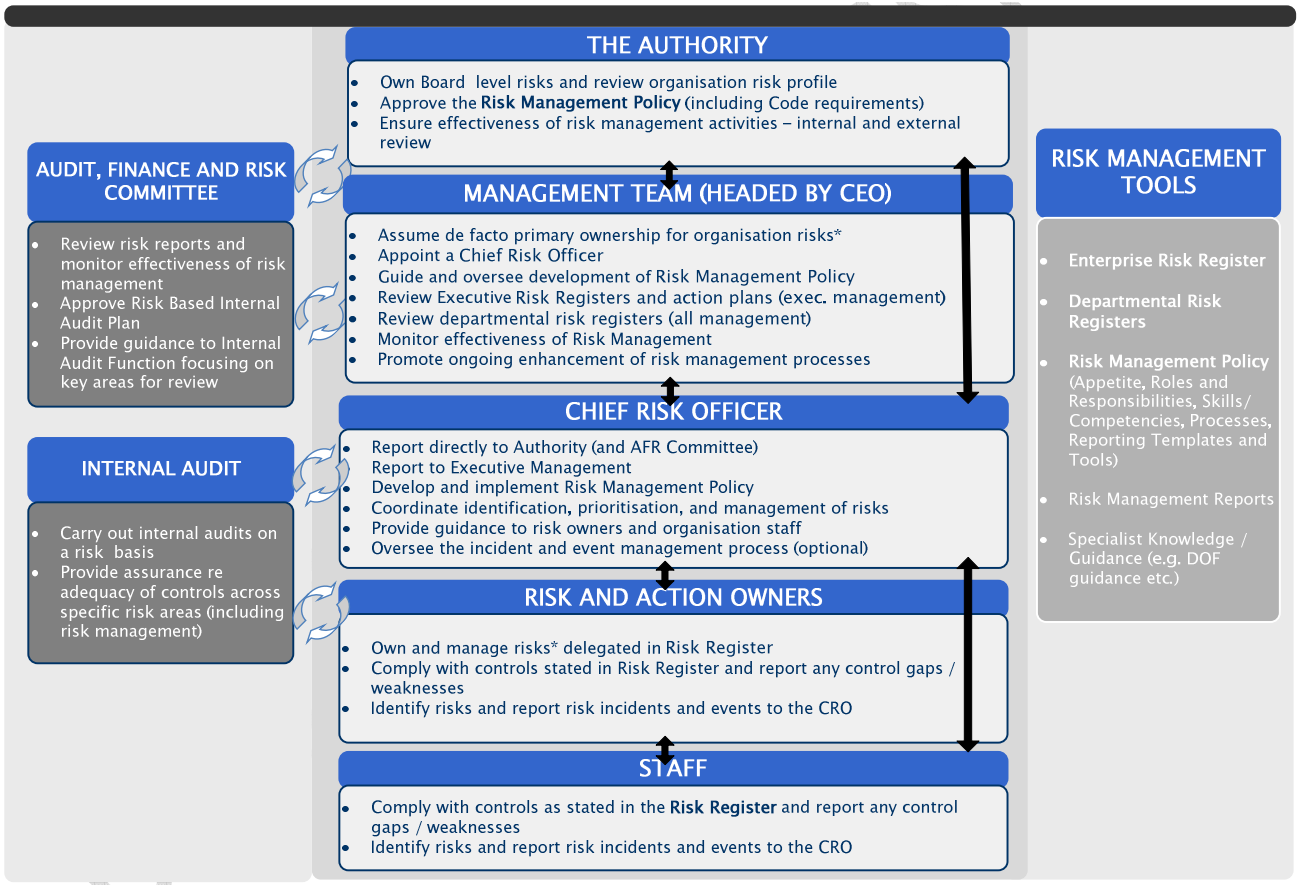
Risk Category	Assessment	Risk Appetite Guiding Statements
Strategic	**Medium Risk Appetite**	The Dublin Docklands Development Authority's mission is to develop the Dublin Docklands into a world-class city quarter paragon of sustainable inner city regeneration - one in which the whole community enjoys the highest standards of access to education, employment, housing and social amenity and which delivers a major contribution to the social and economic prosperity of Dublin and the whole of Ireland. In pursuance of this mission, the Authority must at times accept a level of risk in certain new and unchartered territories. The Authority will take opportunities where considered justified by the potential long term economic and societal rewards. Its risk appetite in relation to certain new strategic and policy decisions is generally **medium.**
Organisational Performance	**Low Risk Appetite**	The Authority recognises that in the current environment organisations are increasingly required to demonstrate value for money and the achievement of organisational objectives. As such the Dublin Docklands Development Authority's appetite for risk in this area is generally **low**

Finance & Funding	**Medium Risk Appetite**	The Authority recognises dynamic management of financial resources is a requirement given the current economic environment and constraints on public funding. As such its risk appetite in relation to allocation of available resources (in the current economic environment) is **medium.** The Authority will however maintain its high financial stewardship standards and will continue to ensure that financial commitments do not exceed available resources. Its risk appetite in relation to financial stewardship is **low.**
Governance, Legal and Compliance	**Zero Risk Appetite**	The Authority defines policies and procedures to support its legal and compliance requirements. The organisation is not willing to accept risks under any circumstances that may result in reputation damage, financial loss or exposure, major breakdown in information system or information integrity. As such its risk appetite in the category of Governance and Compliance is generally **Zero.**
Operational & IT	**Low Risk Appetite**	Operational includes all other operational areas outside examinations including those day to day risks associated with support functions e.g. HR, IT. The Authority has developed a comprehensive and rigorous framework including policies and procedures to support operational management and as such its appetite for risk in this area is generally **low.**
Communication	**Medium Risk Appetite**	Communication relates to risks associated with the provision of information to support Management decisions. Also taken into account here is the risk of negative public perception of the Dublin Docklands Development Authority arising from inappropriate communication with external stakeholders and prevailing perceptions in the media. The Authority's appetite for risk in relation to the public perception prevailing in relation to the Dublin Docklands Development Authority is **medium**.

4 Risk Management Framework

4.1 Overview

Risk management has a better chance of becoming embedded across an organisation if it is operated on the basis of clearly-defined structures and responsibilities. The diagram below presents the high level risk management framework for the Authority.



4.2 Structures and Responsibilities

The roles and responsibilities for each of the groups outlined in the framework diagram above are detailed below:

Structure	Responsibilities
The Board	The Board (Authority) should approve the risk management framework and monitor its effectiveness. It should review material risk incidents and note or approve management's actions, as appropriate. Key elements of the Board's oversight of risk management would include: ▪ Assume ownership of Board level risks ▪ Make risk management a standing meeting agenda item ▪ Consider establishing a Risk Committee / include responsibility for risk in Audit and Risk Committee charter ▪ Include risk management experience/expertise in the competencies of at least one director. Where composition of the Board does not allow for this, expert advice should be sought externally ▪ Approve the Risk Management Policy, set the Authority's risk appetite, and approve the risk management business plan and risk register at least annually ▪ Review management reporting on risk management and note/approve actions as appropriate ▪ Require external review of effectiveness of risk management framework on a periodic basis.
Executive Management (headed by CEO)	Executive Management - consisting of the Chief Executive, and the Senior Management Team – ▪ Assume primary ownership for organisation risks and actions in Risk Register and Risk Business Plan ("Risk Register") ▪ Contribute to the development of Risk Management Policy ▪ Monitor effectiveness of risk management ▪ Promote ongoing enhancement of risk management processes ▪ Comply with controls stated in Risk Register and report any control gaps / weaknesses ▪ Participate in the identification, measurement, prioritisation, and management of risks and controls ▪ Report systematically and promptly to the chief risk officer any perceived new risks or failures of existing control measures ▪ Monitor the effectiveness of risk management ▪ Promote the ongoing enhancement of risk management processes
Chief Risk Officer	The Chief Risk Officer – CEO -should: ▪ Provide guidance to risk owners regarding the identification and management of risks Due to the importance of this role the Chief Risk Officer is the CEO.
Staff	Staff should: ▪ Comply with controls as stated in the Risk Register and Risk Management Business Plan and report any control gaps / weaknesses ▪ Identify risks and report risk incidents ▪ Provide input into the identification and management of risks as required ▪ Understand their accountability for individual risks ▪ Take responsibility for carrying out control activities, reporting on control gaps / weaknesses ▪ Update management regarding status of risks and controls as required
Audit / Finance / Risk Committee	The Audit/Finance/Risk Committee should be responsible for reviewing and agreeing the processes for managing risk. The Committee should have risk management as a standing agenda item at its meetings and should exchange information with the Board, Internal Audit and the Chief Risk Officer regarding the effectiveness of the risk management framework. This role includes: ▪ Review risk reports and monitor the effectiveness of risk management ▪ Approve the Risk Based Internal Audit Plan ▪ Provide guidance to the Internal Audit Function focusing on key areas for review

Structure	Responsibilities
Internal Audit	Internal Audit should: ▪ Provide objective assurance to the Board on the effectiveness of organisation risk management ▪ Help ensure key business risks are being managed appropriately and that the system of internal control is operating effectively

4.3 Risk Register

The risk register should be used as the primary tool to support the formal risk management process in DDDA. The register serves as a useful tool for the Executive Board, CEO, Executive Management and the Audit/Finance/Risk Committee in the tracking and management of key risks impacting the objectives and performance of the organisation, with the risk summary dashboard providing a high level portfolio view of risks.

The register is used to record risks and their associated priority, allocate ownership of the risk to the individual or group best placed to do so, and to identify current controls in place and future actions required to manage risks.

Please note that it is a requirement of the Code of Practice for the Governance of State Bodies 2009 for state bodies to "approve the risk register and business plan at least annually". DDDA have recorded risks, the control in place to manage the risks and additional actions required to improve the management of risks on the risk register and therefore the risk register can also be considered to be the risk management business plan.

The template risk register (also called the risk management business plan) and the risk summary dashboard is included in Annex 5.

5 Risk Management Process

In practical terms risk management involves a cycle of identifying risks, assessing and prioritising the risks and developing action plans to improve how risks are managed. The cycle is completed by a system of regular monitoring and reporting.

On an annual basis (at a minimum) risks are formally identified, assessed and prioritised. Action plans are developed and the results are submitted to the Executive Board and the Audit and Risk Committee along with a report from the Chief Risk officer regarding the overall risk management framework.

The practical aspects associated with each of the four activity areas is presented in further detail below.

5.1 Identify Risks

Risk identification involves summarising the organisations exposure to uncertainty through consideration of the specific factors such as the legal, social, political and cultural environment as well as its strategic and operational objectives. The risk identification process specifically involves consideration of factors that could impact the achievement of strategic and operational objectives.

Risks should be identified across the risk categories outlined in Annex 2.
Guidance on phrasing risks, controls and actions is included in Annex 3

5.2 Assess and Prioritise Risk

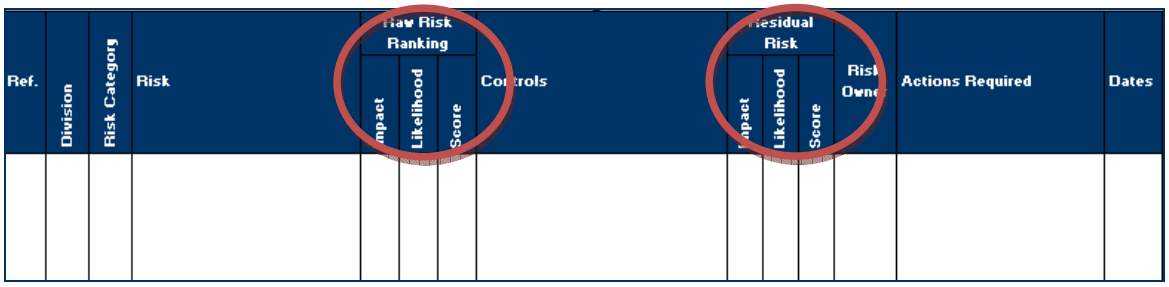
Risks are assessed and prioritised through consideration of:

- **Impact:** The impact on DDDA if the risk actually happens is estimated using a scale of 1 to 10, where 1 is equivalent to having minimal impact and 10 is equivalent to having an extremely detrimental impact.
- **Likelihood:** The likelihood of occurrence is estimated again on a scale of 1 to 10 where 1 is rarely, if ever, and 10 is basically unavoidable/already happening.

A risk score is determined by multiplying the risk likelihood by the risk impact. The risk scores are defined using the well known traffic light system, as follows:

- Low Risk (**L**) 0 – 25
- Medium Risk (**M**) 26 – 50
- High Risk (**H**) 51 – 75
- Extremely High Risk (H+) 76 +

Importantly this prioritisation occurs at two levels as indicated by the red circles in the in the diagram below:



- **Raw risk ranking:** Risks are first prioritised based on consideration of likelihood and impact in the absence of any controls or mechanisms to manage the risk.
- **Residual risk ranking:** Risks are prioritised again, after the controls that are currently in place to manage the risk have been fully considered. The individual assessing the risks determines how well the risk is currently being mitigated and uses the residual risk ranking mechanism to record the results.

5.3 Develop Action Plans

When risks have been identified and assessed, appropriate methods for addressing them should be identified. As such a suite of actions is identified to improve the management of risks. These actions should be expressed clearly on the risk register and assigned an owner and a completion date.

5.4 Monitor and Report on the Management of Risk

Ongoing monitoring of both the management of individual risks and the effectiveness of the overall risk management framework is required on an ongoing basis. All individuals and groups are required to identify and escalate any risk incidents or changes in the risk environment. Those delegated with responsibility for actioning risks, are responsible for ensuring actions are implemented.

Oversight for risks rests with the Executive Board and the Audit/Finance/Risk Committee, who are required to review the report from the Chief Risk Officer, and gain additional assurance that risks are managed appropriately. An example of the template report that the Chief Risk Officer may use to report to the Executive Board and the Audit and Risk Committee is included in Annex IV.

The following are the minimum formal monitoring and reporting requirements required by DDDA

- Update risk register and provide reports to all key management and oversight committees – Once annually
- Review and assess the adequacy of the overall risk framework including the risk appetite statement and structures and responsibilities for managing risk – Once annually

ANNEX 1 – GLOSSARY OF TERMS

- **Risk:** Risk can be thought of as a possible loss or other adverse consequence that has the potential to interfere with an Organisation's ability to achieve its objectives and fulfil its mission

- **Risk Management:** The process by which an organisation seeks to understand its risks and take informed actions to raise the probability of success, reduce the likelihood of failure, and decrease the uncertainty of overall business performance

- **Risk register:** A risk register is the primary tool used by organisations to support the risk management process. It records risks and identifies current controls, allocates ownership of the risk and controls to the individual best placed manage the risk, and identifies future actions for the management of risks. It is also referred to as the Risk Register and Risk Management Business Plan (in the Code for Practice for the Governance of State Bodies 2009)

- **Raw Risk:** The level of risk faced by an organisation before any internal controls are applied

- **Control:** Any action taken to manage risk & increase the likelihood that established objectives and goals will be achieved

- **Residual Risks:** The risk remaining after management takes action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk

- **Action:** Additional checks or safeguards that are required to manage the risk but are not currently in place

- **Risk Ranking:** The suggested risk ranking follows the 3-steps of Low, Medium, and High that can easily be translated into the well-known traffic light system. The ranking is based on the product of impact and likelihood.

- **Risk Appetite:** *"The level of risk that is acceptable to the Board. It may be set in relation to the organisation as a whole, for different groups of risks or at an individual level* [3]*"* or *"the amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time*[3]*"*

- **Summary Dashboard:** provides a summary overview of the number of high, medium, and low risks facing the organisation by category and division

- **Consequence:** is a statement of the impact that the risk would have on the organisation's objectives if realised

[3] The Orange Book: Management of Risk – Principles and Concepts

ANNEX 2 – RISK CATEGORIES

Category	Description	What to include?
Strategic	Risks arising from an absence of high quality Strategy and Business plans	▪ Delivery of efficient and effective service ▪ Achievement of objectives ▪ Monitoring of implementation of Masterplan and related planning schemes
Finance and Funding	Risks associated with the financial stability of the Authority	▪ The Authority as a going concern ▪ Compliance with EU & National Procurement Legislation ▪ Adequate protection of Authority assets in the form of maintenance and insurance ▪ Performance of Authority debtors ▪ Externally imposed delays to planned activities
Organisational Performance	Risks arising from organisational inefficiencies which may impair the realisation of Authority objectives	▪ Monitoring of Organisational Structure and procedures to ensure they are comprehensive ▪ Staffing and Human Resources issues ▪ Disaster Recovery plan ▪ Any action by Tenants and counterparties that is outside Authority objectives
Governance, Legal and Compliance	Risks associated with non compliance on the part of the Authority with its legal and policy obligations	▪ On going revision and implementation of Corporate Governance Policies ▪ Risks of litigation against the Authority
Operational & IT	Risks arising from day to day activities of the Authority	▪ Adequate IT systems to manage information and documents necessary in decision making ▪ Security of sensitive data
Communication	Risks associated with the provision of information internally and externally and the resulting public perception of the Authority	▪ Provision of information to support Management decisions ▪ Communication with external stakeholders

ANNEX 3 PHRASING OF RISKS, CONTROLS AND ACTIONS

The general principle is that risks and associated controls and actions should be presented and phrased in such a way as to be clear to all readers/stakeholders including staff, the chief risk officer, the management team, internal audit, the Audit and Risk Committee and the Executive Board. It is best to make the risks as specific as possible – in principle risks that are too far reaching, are unwieldy and difficult to action. Some additional specific guidance is included below.

Risks

Risks should be clearly expressed and the structure of the risk should clearly state:

- Vulnerability
- Consequence
- Impact

E.g. Risk that X occurs, as a result of Y, leading to Z

Controls

Controls should be easily understood and should clearly demonstrate the checks or safeguards in place to manage risk. Controls are only to be included if they ***are currently*** in place i.e. as distinct from planned actions.

Actions

Actions should only be included if they are:

- Additional checks or safeguards that are required to manage the risk but are ***not currently*** in place
- Tangible i.e. the action is clear and capable of implementation and tracking

ANNEX 4: EXAMPLE REPORT

Report from the Chief Risk Officer to the Audit / Risk Management Committee

1. Introduction

The purpose of this document is to:

- Inform the Risk Management Committee about the ongoing management of risks at departmental level
- Formally communicate any issues impacting the organisations risk environment to the Risk Management Committee.

2. Overall Performance of the Business Unit

Guidance: *Include high level details as appropriate. The content and level of detail should be consistent with other management reports used to monitor overall effectiveness.*

3. Significant Events Impacting the Risk Environment

Guidance: *For example significant staff changes in this area or incidents & problems that occurred in the past 12 months.*

Event Dashboard		
Description of event	**Comment / action plan**	**RR updated (Y/N)**

4. Overview of additions / changes to the Risk Register

Division	Prior Period			Current Period			Total Prior Period	Total Current Period	Variance
	H	M	L	H	M	L			

Report from the Audit/Finance/Risk Management Committee to the Board

1. Introduction

The purpose of this document is to:

- Document any changes in the strategic risks facing the organisation
- Formally communicate any issues impacting organisation's risk environment to the Audit Committee and the Board

2. Overall Performance of the Organisation

Guidance: Include performance against strategic objectives etc

3. Significant Events Impacting the Risk Environment

- Organisational or External Events
- General Events: As per the Chief Risk Officer Report

Event Dashboard		
Description of event	**Comment / action plan**	**RR updated (Y/N)**

4. Overview of additions / changes to the Risk Register

Division	Prior Period			Current Period			Total Prior Period	Total Current Period	Variance
	H	M	L	H	M	L			

5. Risk Dash Board

The following table shows the high level risks as identified within each section as of DD/MM/YYYY.

High Level Risks as of DD/MM/YYYY		
No.	**Risk**	**Action Plan**
1		
2		
3		

6. Other Comments or issues in relation to the Risk Management Process

7. Prepared and approved by (Members of Risk Management Committee)

Date: _____

Name: _____

Date: _____ Name: _____

Date: _____

Name: _____

ANNEX 5 – TEMPLATE RISK REGISTER AND EXAMPLE SUMMARY DASHBOARD

Note: These are templates only – the Chief Risk Officer is responsible for maintaining the most up to date documents.

Ref.	Division	Risk Category	Risk	Raw Risk			Controls	Residual Risk			Risk Owner	Actions Required	Dates
				Likelihood	Impact	Ranking		Likelihood	Impact	Ranking			
1	Information Technology	Operational	Risk that the organisation fails to adequately safeguard data stored on laptops, leading to sensitive information being inappropriately accessed / used	8	8	H	An IT Security Policy is in place All laptops have been encrypted	5	8	M	Head of IT	Head of IT to commence a project to achieve ISO 27001 and IS0 27002 compliance within a one year period	Q1 2010
2	Corporate Services	Compliance	Risk that the organisation fails to comply with health and safety requirements, leading to a breach of legislation and possible litigation	6	3	L	Health and safety policy in place Health and safety training provided to all staff	6	3	L	Head of CS	No Actions Required	