

# Coast to Capital

**Meeting:** Coast to Capital Audit Committee Meeting  
**Date:** 13 November 2019  
**Report Title:** Corporate Risk Review  
**Report by:** Cali Gasson – Investment Programme & Risk Manager, Coast to Capital  
**Item No:** 2  
**Part:** A

---

## Recommendation:

The Audit Committee is asked to:

- Recommend the Board to approve the risk management framework and policy following the review conducted by BDO.

### 1. Context

BDO have been reviewing the risk management processes at Coast to Capital and have set out a new risk policy, which will update the current way of working in line with our changing operating environment.

This review has seen BDO conducting various sessions and workshops to engage with Board members, SMT and other key internal individuals to determine Coast to Capital's risk appetite to inform a new risk management process including the governance of risk.

A Risk Policy has now been developed that demonstrates a process and framework, to include a recommended risk appetite that will enable specific tolerance levels to be set. In addition BDO are currently working through identifying risks and developing a new company and departmental risk registers, which will be implemented in early 2020.

The Audit Committee are asked to review the Risk Policy Document in **Annex A**, and recommend that the Board approve the policy document at the January meeting.

### 2. Diversity Statement


There are no diversity impacts to consider on this paper.

### 3. Legal Statement

No legal position has been sought on this paper.

## Annexes (Part A)

- **Annex A:** Risk Policy



**Efficiently owning,  
operating, and  
embedding our approach  
to risk.**

## Introduction – what is a risk?

- 1 A risk is defined as a threat to achieving a business objective. The threat can be directly related to the various programmes Coast to Capital grant fund, support functions such as IT, human resources and finance and risks affecting us that arise from elsewhere – from our clients, third parties, suppliers, regulators and their requirements, from our competitors, the economic climate, political risks, and so on. Risk also relates to opportunities – which enables an objective to be met more completely, more quickly, with more impact or more cheaply, with less collateral adverse impact. Overall, however, risk is about uncertainty: a risk that has crystallised is an issue.
- 2 This risk policy explains Coast to Capital's policy, attitude, management processes, and appetite for risk. It is formally endorsed and signed off by the Board and applies to all staff. A risk policy, however, should go beyond the production and approval of a policy document: it should be reflected in the active processes and culture of the organisation.
- 3 The risk policy is intended to minimise the company's risks to achieving its business objectives, to a level which, ultimately, the Board is prepared to accept or tolerate. It means that the Board's decisions may involve a degree of business risk, but the decisions and actions that follow, are undertaken in a managed way, with due consideration of risk before the decision is made and with due consideration of the regulated environment in which the company operates.
- 4 The Board ultimately owns and is responsible for the risk management processes in Coast to Capital. The Risk Manager, and specific risk leads in each department, helping to facilitate the process and advising the Executive Committee, Audit Committee and Board on the process, its effectiveness and the risks.
- 5 Risk is considered in business planning, the development of business cases, day to day monitoring of operations, key performance measurement and project management activities, and part of the selection and oversight of business partners and suppliers.
- 6 The purpose of risk management is to ensure that Coast to Capital carries out its business in a way which avoids unnecessary risk to the:
  - ability to achieve business objectives,
  - reputation and standing with governments (local & national), business partners, stakeholders and the communities Coast to Capital operate within,
  - operational effectiveness,
  - financial standing or company assets,
  - ability to comply with statutory and regulatory obligations, or

- avoids unnecessary risk to public finances within its risk appetite and tolerance framework, the health, safety and wellbeing of staff and partners', stakeholders, employees and contractors.
- 7 However, risk management is not purely in place for regulatory purposes or preparing the company regulated environments in the future – it is a part of good management practice that operates throughout the organisation. Nor is risk management purely about the 'down side': risk is also about exploiting opportunities. Nonetheless, the risk policy helps to protect company reputation, respond to problems quickly, leads to fewer surprises, and helps develop a firm foundation for success.
- 8 This risk policy applies to all Coast to Capital activities and parts of the business. Consideration of the risks to Coast to Capital includes risks that are caused by factors within the organisation, suppliers, partners, those relating to company activities, and those risks caused by external factors.

## Methodology

- 9 The method is described in full below and summarised in Appendix A.
- 10 We use a standard methodology and terminology to identify and assess risks:
- **Identification** – Coast to Capital identifies the risks through a comprehensive consideration of the key risk areas affecting a typical Local Enterprise Partnership model and its explicit and implicit key objectives, mission and values. Identification is achieved through periodic reviews of key risks, providing the various levels of staff with the opportunity to flag risks to be included. This process of identification is owned and supported by the Risk Manager. It is, however, the responsibility of all staff and stakeholders, whatever their position, to identify risks. Risks are identified through several activities which are outlined in the table below:

Business activity	Risk activity	Outputs
Strategy formulation and business planning	Integral to strategic and business planning, Coast to Capital takes stock of its activities, risks and core purpose, identifying risks which impact on its core purpose and mitigations that require investment.	Core risk register is fundamentally refreshed. Key risks and mitigations included in corporate strategy and latter business plans.
Personal staff development plans and objective setting	Consider risks and any objectives that staff should consider as risk	Personal development plans have risk element.

	management responsibilities re risk (e.g. risk process role or specific mitigations).	
--	---------------------------------------------------------------------------------------	--

- Ownership** - Each risk identified is assigned an owner who is regarded as the lead person accountable for ensuring that the risk is being managed. The owner of the risk may not be the owner of the current mitigations in place or future mitigations planned to be put in place, but have the overall accountability for the management of the risk. The CEO does not own most of the risks, even though is ultimately accountable for all of the risks' management. The Senior Management Team, supported by the Risk Manager and Risk Leads, does not own all of the risks: the risks are the responsibility of line management and, ultimately, the Board collectively.
- Assessment** - Not all risks are as important as others. The company assesses or scores the risks based on a perceived likelihood of the risk occurring and the impact if the risk were to occur. We assess the risk both before taking account of the key mitigations or controls (called the inherent risk) and again after those controls are taken into account (called the residual risk). We are thus able to establish the importance of the risk and focus on the risks that are more material to us.
- Coast to Capital *assesses* the risk using a five-point scale for likelihood and impact using the terms in the diagram below. The terms are explained in more detail in Appendix B. We combine the likelihood and impact to gain an overall risk assessment, which is the multiple of the likelihood and impact scores. We use generic terms for each point on the scale so that Coast to Capital can compare the wide variety of risks that Coast to Capital face using a common point of reference.
- Coast to Capital pre-define its **risk appetite** by attributing the appetite level to a given *residual* risk combined score. The company uses a traffic light system to indicate whether a risk is within tolerance (green); outside of tolerance (amber); significantly outside of tolerance (red). The table shows the tolerance level for a given combined residual risk score in a 'heat map'.

## Risk heat map

4 - Almost Certain	4	8	12	16
3 - Probable	3	6	9	12
2 - Possible	2	4	6	8
1 - Unlikely	1	2	3	4
	1 - Minor	2 - Moderate	3 - Major	4 - Catastrophic

- We note if the risk is likely to be getting more or less severe – called the risk ‘dynamic’. This gives readers of the register an indication of whether the situation is likely to improve over time, is stable, or is likely to be deteriorating in the near future.
- A risk outside of tolerance requires an improvement in internal controls or mitigations or, at the extreme, the termination of the activity altogether. These are actions for improvement, which are recorded in action plans, should include defined deadlines and owners.
- Red risks generally require higher priority actions, although red risks may involve significant investment to put right or significant time to bring under adequate control. There may be interim solutions available to mitigate or part-mitigate the risk in the short term while the longer term fix is being developed. Ultimately if a red risk cannot be mitigated the activity may need to be discontinued, if possible.

## Recording of risks

- 11 Risks are recorded in one risk register which is administered day-to-day by the Risk Manager and risk leads in each department. The register is held electronically in a spreadsheet held by the Coast to Capital’s Risk Manager. Each department has its own risk register, with the top risks being transferred onto the company risk register.
- 12 It is the responsibility of the Risk Manager, supported by the Risk leads for each department, that the register is reviewed by risk owners and kept up to date to the prescribed frequency. The leads responsibilities are to facilitate the process of update, including holding meetings with staff to discuss their risks.

## Reporting

- 13 The top 20 or so company risks are presented by the Risk Manager at the Executive Committee meetings (ExCo) bi-monthly for their consideration and review. The exact number of risks in the top category can vary, but 20 is an indicative maximum level, the 'top 20' reference is used throughout this policy as a shorthand for the top company risks. Also, the frequency distribution of the entire risk register and the major movements and trends since the previous ExCo meeting is recorded and reported. The risk report to ExCo explains the movements in risk since the last review and the review process undertaken in the period up to the publication of the risk report.
- 14 It is the top 20 or so risks that are reported to the Audit Committee. The Board receives and reviews the top 10 of those 20 risks. Each department will retain its own risk register with around 20 risks as a maximum (excluding Investments), which would also include risks that are in part or wholly managed by those department heads which fall within the company top 20 risks.
- 15 The ExCo top 20 company risk register and the statistics on the rest of the register are reported to ExCo first and then presented to the Audit Committee by the Risk Manager after ExCo and CEO have reviewed the register, adding any further commentary, and making any updates. Risk reporting to the Board is conducted at every meeting, with a full report and update taking place annually.
- 16 In order to ensure that risk is properly integrated into business performance and to provide an indicator of organisational and programme delivery health, risk indicators (the top risks, current residual score levels and progress against actions) are provided as part of normal company reporting, alongside financial and delivery performance. Any notable points and changes since the last reporting period and likely forthcoming changes, are duly noted in a brief narrative.

## Monitor and review

- 17 In overall terms, risks are monitored and reviewed every month by the risk leads in each departmental, prior to their reporting to the Risk Manager. Review of the risks involves the re-evaluation of the risk 'title', its likelihood and impact, an assessment of the controls or mitigations and the progress of actions. Monitoring is ensuring that the risk management process is being carried out and the output and activities are sensible and proportionate. This is conducted in each department's regular team meetings. It can be facilitated by the Risk Leads through individual meetings and then discussed and approved by the department heads



- 18 Significant risks emerging from the departmental review process are reported specifically as potential 'promotions' to the company risks. To ensure adequate embedding of risk management, the departmental risk register should form the first item on the agenda of a departmental team meetings. Any amendments (or additions or deletions) to risks, risk assessments, assessment of mitigations, progress of any actions, gets documented in the departmental register updated. The key to integration is that the risk register is a regular discussion point and a tool to drive business review and reporting.
- 19 ExCo review the output of the review process bi-monthly, as a standing agenda item at their formal meetings. Their focus is on the company risks (top 20) to Coast to Capital to include an examination of key risks coming out of each department and consideration of any risks identified by ExCo members themselves.
- 20 The Audit Committee reviews the top 20 (company) risk register. Its role is to review the effectiveness and efficacy of the document and underlying processes prior to the Board conducting their assessment. It can call on departmental leads to present on those lead risks and activities as a means to providing additional assurance. The Audit Committee thus provides the role of assurance on the process of risk management, and through that, the content of the register. The Audit Committee give assurance to the Board that they have undertaken this review, as part of its report to the Board on the outcome of the Audit Committee's deliberations and scrutiny. The Audit Committee may challenge management's interpretation of the risks, risk assessments and progress of recommendations in the register. The Audit Committee may engage internal auditors or other independent persons to review the risk management process and the management of individual mitigations of risk.
- 21 The Audit Committee reviews the risks on a 6-monthly basis or whatever its meeting frequency, once ExCo review has been completed and any ExCo amendments are incorporated. Views of Audit Committee on risks are taken into account during Audit Committee discussions and can influence the assessment of the risks, the risk titles and the mitigations required.
- 22 Changes required by ExCo, the Board or Audit Committee are then cascaded down to the relevant departments for action. Thus, Coast to Capital's review and monitoring of risks is both 'bottom up' and 'top down'.

### Company risks

- 23 Company risks are the top 20 risks which are inherently the most significant risks to the company and are likely to create a significant impact on the company's overall ability to deliver its objectives or maintain its standing and reputation. ExCo agrees on what the

company top 20 risks are, based on its own assessment from its perspective to include key risks identified by the departments.

- 24 The focus of ExCo and the Board review is the strategic risks, the top 20 risks for ExCo and Audit Committee; and the top 10 of those are the main focus of the Board.

### Refreshing the risk identification and assessment

- 25 Every two or three years or so, Coast to Capital takes a strategic review of its risks with special workshops at Board, senior ExCo and departmental head level. The last fundamental review took place in September 2019.
- 26 Breaches, incidents and losses and control arrangements can be recorded and linked to the register.

### Risk Appetite Statement

- 27 The risk appetite is the assessment of the risk that the company is prepared to take tolerate in order to pursue an opportunity. The risk appetite varies on the type of risk and the level of exposure that might crystallise if an opportunity were to be pursued. The company has taken the view that its risk appetite can be grouped with similar risk.
- 28 The risk appetite is given in a statement and reviewed by ExCo and then the Audit Committee once a year.
- 29 The risk appetite is summarised in Appendix C.

### **Risk of third party providers, grantees, partners and suppliers**

- 30 Coast to Capital uses external suppliers and partners to support its key functions – across all of its grant funded projects and the office support functions. Risk management should extend to the risk management of these external parties. This is achieved through: one, the selection of grantees, partners and suppliers who demonstrate good risk management credentials; secondly, monitoring the partners and suppliers carefully and, thirdly, ensuring risks relating to the services outsourced are fully understood and managed by the suppliers and Coast to Capital. Significant partners should be demonstrating their risk management and can be allowed limited access to Coast to Capital’s risk register for this purpose.

### **Business cases, business planning and other decision-making**

- 31 The primary risk management policy and activity is the regular review and update of the risks in the company’s formal risk register spreadsheet.
- 32 However, for key business decisions, a brief risk assessment should also be undertaken and recorded prior to the decision to commence the activity or venture. Business decisions bringing high commercial return may carry a high degree of inherent risk – both threats and opportunities. However, new activities or ventures can be made less risky, with the consideration of suitable controls in place to maximise the outcomes from the business decision.

### **Projects**

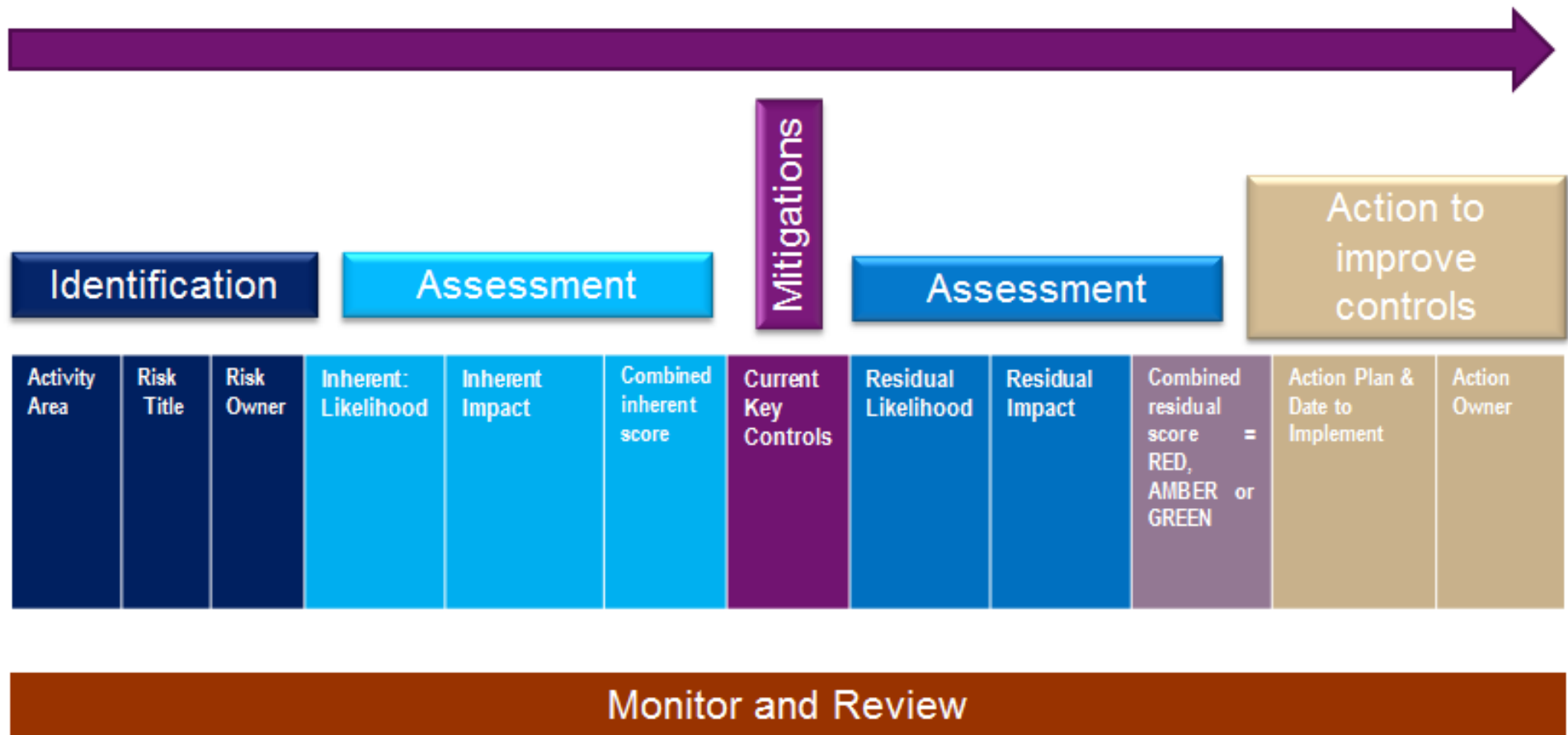
- 33 It is good practice to capture project risks. These can be captured using the same risk capturing tools used for the company risks. Significant project risks can be escalated if required, by giving them a high score and flagging them as project top risks. It is important that significant project risks (internal projects and those funded by Coast to Capital) are fully integrated into Coast to Capital’s formal risk management process. In many cases, such risks are going to be significant risks to the organisation and the success of the company’s strategy.

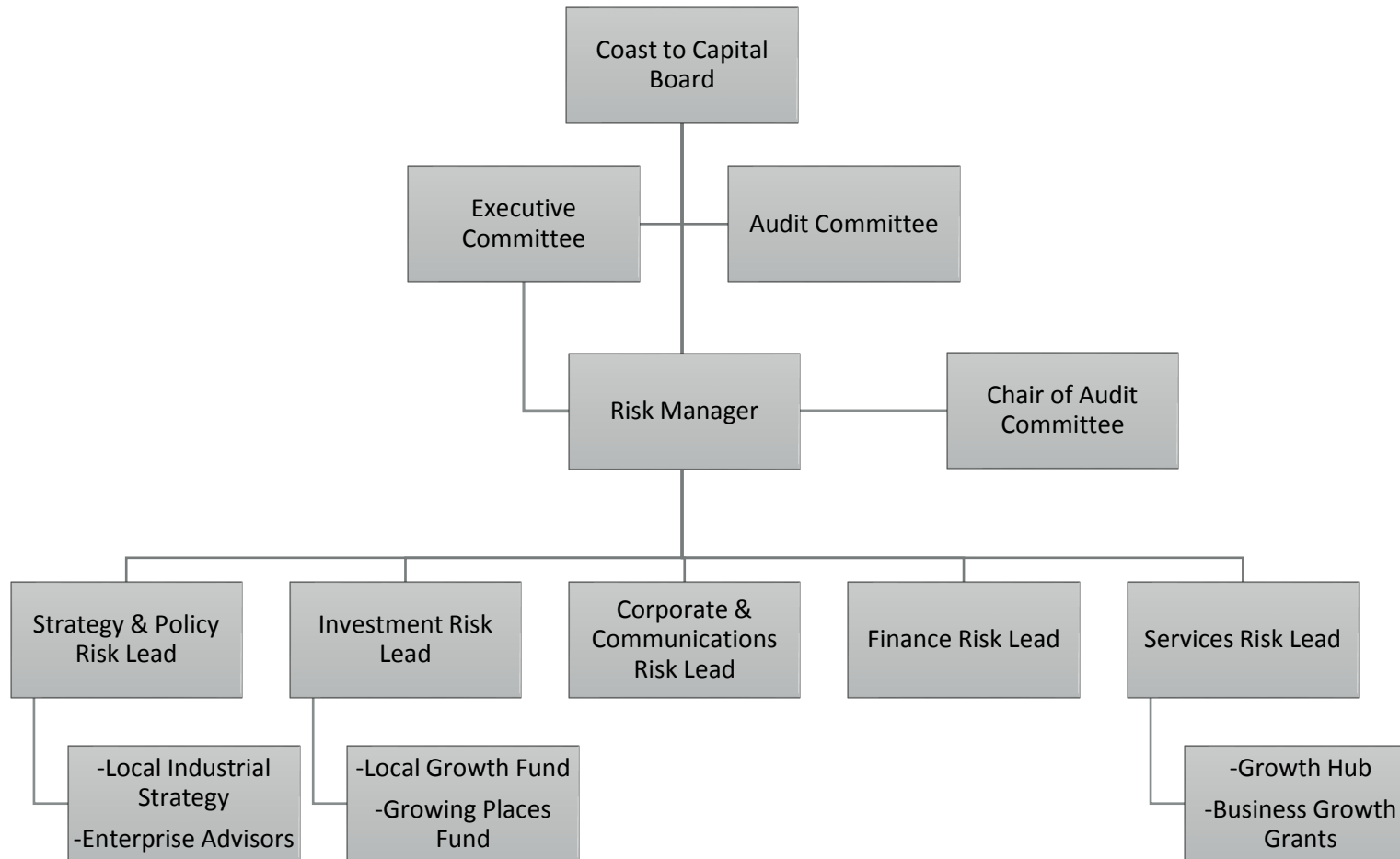
### **Health, Safety and Environment risks (H&S)**

- 34 Health, safety and environment risks can be captured using current systems designed for those purposes. For example, risk assessments for home working or travelling on business should continue to use H&S risk assessment procedures. Significant health, safety and environmental risks should be recorded in the main company risk register and can be linked to strategic or top operational risks on health, safety and environmental.

Appendix A: Risk Management Policy Summarised

Risk review cycle





## Appendix B: Impact and Likelihood Definitions

### Impact

Defined as the **impact** or consequence of the risk if it were to occur. The impact can be ONE or more of the following:

- 4 - Catastrophic**
  - An incident so severe in its effects that a key operational service or project will be unavailable permanently or a significant time (weeks/months)
  - Strategic objectives set are not met
  - Statutory duties are not achieved
  - Death of an Employee, contractor, or Member of the Public
  - Financial loss over three month operating loss ; fraud loss of greater than £50,000 (£100,000 for fraud with projects, cumulatively or individually)
  - Adverse national media attention - National televised news report, likely to be sustained over a long period of time
  - Litigation almost certain and difficult to defend
  - Breaches of Law or regulation punishable by imprisonment or leading to significant reputational damage or removal of 'licence to operate'
  - Unlikely to recover from any of the above incidents corporately
  
- 3 - Major**
  - Temporary loss of a key service for few days
  - Objectives of a Group/Division are not met
  - Non-statutory duties are not achieved
  - Permanent injury to an employee, contractor or member of the public
  - Financial loss over £100,000 other than fraud; Fraud loss up to £10,000 individually.
  - Adverse localised media attention or high profile attention which is to be not sustained
  - Litigation to be expected
  - Breaches of law or regulation punishable by fine only and consequent reputational damage.
  
- 2 - Moderate**
  - Loss of a key service for a few hours or major depletion of a service
  - Objectives of the Division are not met
  - Injury to an employee or member of the public requiring medical treatment
  - Financial loss over £10,000 other than fraud; Fraud loss up to £5,000 individually
  - High potential for a complaint litigation possible

## **1 - Minor**

- Breaches of regulations/standards
- Depletion of a service or brief service outage
- Objectives of the Activity are not met
- Injury to an employee or member of the public requiring onsite first aid
- Financial loss over £1,000 other than fraud; Fraud loss below £100.
- Minor adverse localised media attention
- Breaches of local procedures/standards
- Unlikely to cause complaint/litigation

## **Below this level**

- Little visible service impact
- Objectives of the individual are not met
- No injuries
- Financial loss between £0 – 999; minor fraud loss.
- No media attention
- No breaches in working practices; No complaints/litigation

## Likelihood

The **likelihood** of the risk occurring *without taking account of mitigations already operating*.

<b>4 - Almost Certain</b>	1 event in 1-2 years) Almost Certain
<b>3 - Probable</b>	(1 event in 5 years), Probable
<b>2 - Possible</b>	(5 to 10 years), Possible
<b>1 - Unlikely</b>	(10 or above) Unlikely

*Tip: **Inherent Risk** assessment is arguably an artificial assessment of likelihood, because it may not relate to the current situation, where mitigations may be in place. The reason for considering inherent risk is to ensure that the importance of the threat is considered first. If the threat was inherently not significant, why bother to control it?*



## Appendix C: Risk Appetite

### Risk Appetite - A Common Currency

Description	Appetite term
Encouraging innovation, offers substantial rewards for innovation which has to be set against the risk of the approach and a higher likelihood that the opportunity will not crystallise	HUNGRY
Open to all different routes to delivery of strong outputs, with some risk of adverse impact attached	OPEN
Moderate levels of risk exposure, preferring acceptable albeit possibly ambiguous output	MODERATE
Accept some low risks, assured delivery route, restricted reward	CAUTIOUS
Accept little risk as reasonably possible, strongly assured options, low chance of adverse outcome, but limited reward.	AVERSE

### Risk appetite

Risk category	Appetite Currently?	Appetite Ambition?
External project financial loss (except fraud)	CAUTIOUS	MODERATE
Internal operations financial loss	AVERSE	AVERSE
Fraud (internal or external)	AVERSE	AVERSE
Reputational impact & 'licence to operate'	CAUTIOUS	MODERATE
Conflict of interest	CAUTIOUS	CAUTIOUS
Investments e.g. LGF	MODERATE	HUNGRY
Loans	OPEN	HUNGRY
Harm to people (staff, visitors, etc.)	AVERSE	AVERSE
Loss of operation	CAUTIOUS	CAUTIOUS
Legal risks, including liability exposures	CAUTIOUS	CAUTIOUS
New ventures and approaches - potentially high impact projects	HUNGRY	HUNGRY

Risk appetite links directly into the description of the impact scores in the risk assessment. Thus, as an example, a financial fraud, have an adverse appetite rating, would mean a fraud value of £10,000 would have a similar level of impact on the 1 to 4 scale as an external investment loss of £100,000 that was not attributable to fraud.