INVEST NI

RISK MANAGEMENT STRATEGY AND POLICY

Version Control

Version: 1.0
Issue Date: 6th October 2017
Approver: Carol Keery
Status: Approved
Next Review Date: 30th September 2019

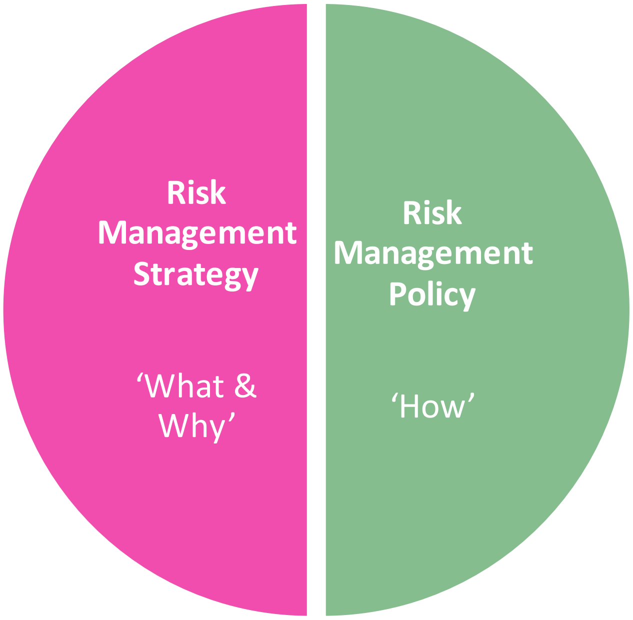
Version	Author / Reviewer	Issue Date	Reason for change	Next Review Date
1.0	Colin Morelli	06/10/2017	First Publication; amalgamation of Risk Management Strategy and Risk Management Policy; revised Privacy Risk section to reflect GDPR and removal of Privacy Impact Assessment screening questions (previously at Annex A); other minor clerical amendments	30/09/2019

CONTENTS

1.0 INTRODUCTION

1.1 Purpose

The purpose of this document is to outline an overall approach to risk management that addresses the risks facing Invest NI in pursuing its mission, vision and aims and which will facilitate the effective recognition and management of such risks going forward ('Risk Management Strategy'). The document also outlines the policy and processes that are used in the management of risk and the structures through which risk is communicated and reported ('Risk Management Policy').



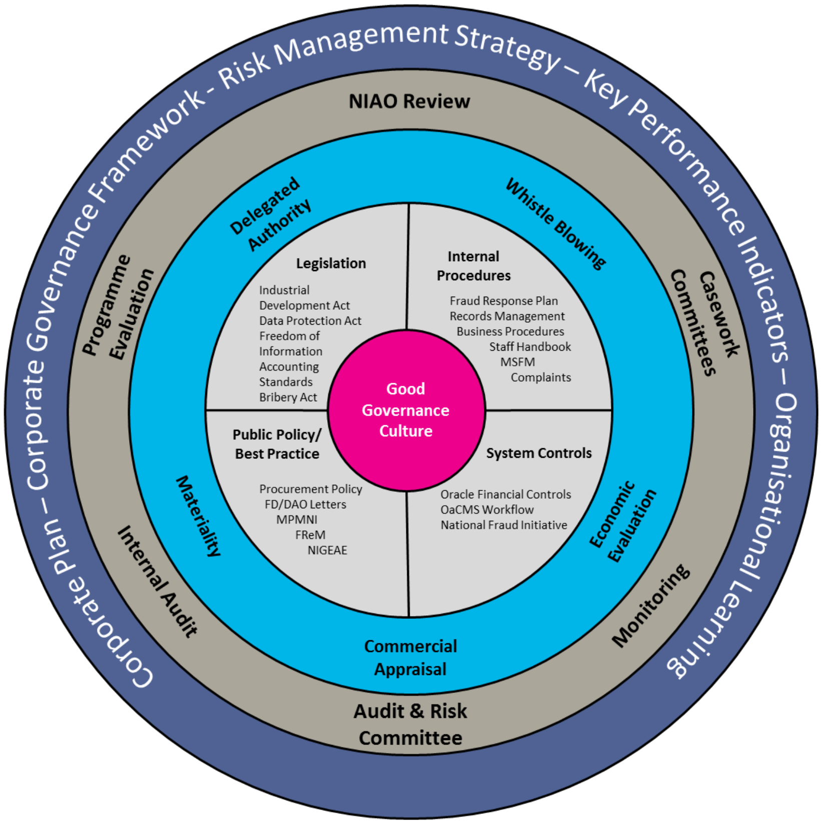
1.2 What is Corporate Governance?

'Corporate Governance' is the system by which an organisation is directed and controlled at its most senior levels in order to achieve its objectives and meet the necessary standards of accountability, probity and openness.

In its simplest form it is about:

ensuring that the right thing is done, in the right way, for the right people, in an open, honest and transparent manner

Feeding through all management levels within the organisation, internal control is fundamental to the management of risk. A sound system of internal control depends upon thorough and regular evaluation of the nature and extent of risks to which the organisation is exposed. The diagram below illustrates the Invest NI Control Environment, to which Risk Management is crucial.



Invest NI Control Environment

1.3 What is Risk Management?

Risk is the possibility of an event or activity impacting adversely on an organisation, preventing it from achieving organisational objectives and outcomes. It includes consideration of what, when, where and how events could prevent, degrade, delay or enhance the achievement of organisational objectives.

Risk is the chance of something happening that will have an impact on Invest NI's business or objectives

Risk management comprises the activities and actions taken to ensure that an organisation is conscious of the risks it faces, makes informed decisions in managing these risks, and identifies and harnesses potential opportunities. Managing risk well requires careful consideration of the key concepts of minimising loss, maximising opportunity and preparing for uncertainty. Risk management can be used to provide a strategic approach to decision-making, which can assist organisations in improving performance and delivering key outcomes more effectively.

The process of identifying and managing risk is to *increase the probability of success* and *reduce the opportunity of failure*

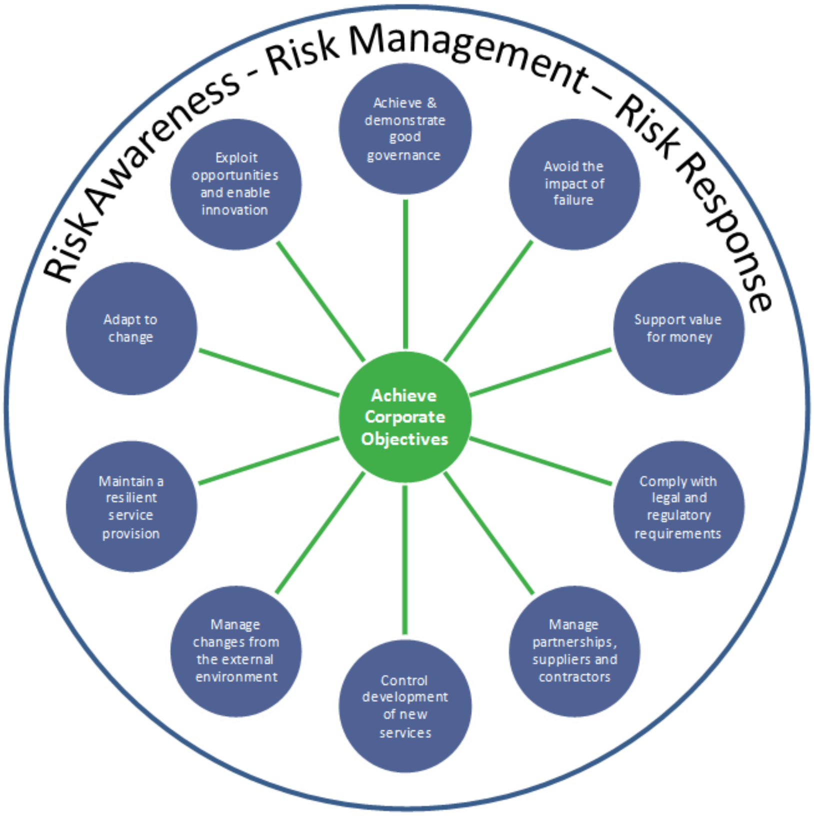
1.4 Why Manage Risk

Through understanding and managing risks, decision-makers will be better able to evaluate the impact of a particular decision or action on the achievement of Invest NI's objectives, thus ensuring:

- Achievement of Corporate Priorities, Targets and Outcomes;
- Efficient, effective and Value for Money service delivery; and
- Innovation is encouraged in a controlled environment.

When embedded within the existing planning and decision making process, risk management:

- Provides the basis for ensuring implications are thought through;
- Ensures that the impact of decisions, initiatives and projects are considered and that conflicts are balanced; and
- Ensures that potential damage attributable to control failures are minimised.


Risk Awareness - Risk Management – Risk Response
Achieve & demonstrate good governance
Avoid the impact of failure
Support value for money
Comply with legal and regulatory requirements
Manage partnerships, suppliers and contractors
Control development of new services
Manage changes from the external environment
Maintain a resilient service provision
Adapt to change
Exploit opportunities and enable innovation
Achieve Corporate Objectives

Benefits of Risk Management

1.5 Application of the Policy

Risk assessment should be included as a routine element of policy development, implementation and project/programme management across the organisation. As such this Policy should be applied, to varying levels, to all aspects of Invest NI's operation.

2.0 RISK MANAGEMENT STRATEGY

2.1 Overview of Risk Management Strategy

In line with best practice principles Invest NI is committed to the implementation of a process for identifying, evaluating and managing risk, whilst also ensuring that the process is regularly reviewed for continuing relevance and effectiveness. If fully implemented, risk management should be embedded within the daily operation of the organisation, from strategy formulation through to business planning, processes and its day-to-day activities.

In developing this Strategy, Invest NI has incorporated good practice obtained from sources such as:

i. HM Treasury Orange Book and related guidance;
ii. Department of Finance (NI) publications;
iii. Seeking advice and guidance from Northern Ireland Audit Office, including their Good Practice in Risk Management publication; and
iv. Process Benchmarking with other Invest NI Public Sector Organisations.

It is important that the Risk Management Strategy does not focus upon risk avoidance but on the identification and management of an acceptable level of risk.

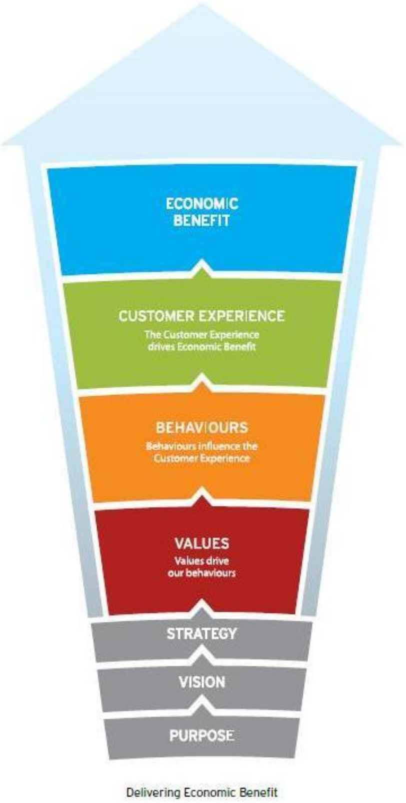
2.2 Policy Statement on Risk Management

Invest NI's policy is to **adopt best practice** in the identification, evaluation and cost-effective **control of risks**, to ensure that they are either **eliminated or reduced to an acceptable level**.

Risk can never be eliminated completely. All staff must understand the nature of risk and accept responsibility for risks associated with their area of authority. The necessary support, assistance and commitment of senior management will be provided to facilitate this.

2.3 Link to Corporate Strategy

As the economic development agency for Northern Ireland, Invest NI's role is to support local business to innovate and grow their exports, and to attract new inward investments. The Business Strategy for 2017-2021 sets ambitious objectives through which Invest NI will deliver outcomes that are aligned with the Northern Ireland draft Programme for Government and the associated Industrial Strategy (Economy 2030). In order to do so, we must accept that many of the decisions taken for the good of the economy must carry with them an associated risk.


ECONOMIC BENEFIT
CUSTOMER EXPERIENCE
The Customer Experience drives Economic Benefit
BEHAVIOURS
Behaviours influence the Customer Experience
VALUES
Values drive our behaviours
STRATEGY
VISION
PURPOSE
Delivering Economic Benefit

As the very nature of our business and the challenges faced within our economic environment dictate that our investments can attract a higher level of risk, it is extremely important that in working towards our objectives we are open to some level of risk and that all members of staff can recognise whether that risk is acceptable given the potential rewards that success could deliver, and manage it responsibly in line with corporate policy.

This trait is reflected in the Values & Behaviours that are expected of all staff, and in particular the 'Integrity' that is expected:

PROFESSIONAL
PASSION
ONE TEAM
PERFORMANCE
RESPECT
INTEGRITY
CUSTOMER FOCUS

Integrity
We take responsibility for all our actions,
in particular the management of risk, and are vigilant in managing public money.
We are honest and fair with each other and our customers (stakeholders)

Therefore our success, and that of the NI economy, is reliant on the implementation of appropriate risk management processes and skills, and an understanding of the impacts risk can have on what we do, both operationally and in the running of the organisation.

2.4 Aims & Objectives

The Invest NI Risk Management strategy aims to:

- Integrate risk management into the culture of the organisation;
- Manage risk in accordance with best practice whilst ensuring best value;
- Ensure compliance with legal and regulatory requirements as an absolute minimum;
- Reduce the overall cost of dealing with risks that have come to fruition (both financial and reputational) and maximise the benefit of opportunities;
- Anticipate and respond to changing social, political, environmental, technological and legislative requirements; and
- Raise awareness of the need for risk management and provide clarity on how risk is to be approached and managed

This will be achieved by:

- Establishing clear roles, responsibilities and reporting lines within Invest NI for risk management;
- Embedding risk management into organisational decision making processes, service delivery, project management and partnership working;
- Providing opportunities for training and shared learning on risk management across the organisation, including Board Members and partners;
- Offering a framework to identify priority risk areas, including the provision of risk registers at strategic and operational levels;
- Reinforcing the importance of effective risk management as part of the everyday work of employees;
- Incorporating risk management considerations into all levels of planning;
- Monitoring of arrangements on an ongoing basis by management;
- Holistically reviewing the organisational risk profile on a regular basis;
- Ensuring robust Business Continuity arrangements are in place;
- Implementing best practice risk management arrangements in accordance with the core Controls Assurance Standards (Corporate Governance, Risk Management, Financial Management, ICT, Records Management & Health & Safety); and
- Independently validating Risk Management processes within the organisation to ensure they are robust and in line with best practice.

3.0 RISK MANAGEMENT FRAMEWORK

3.1 Three Lines of Defence

It is generally considered that there are three main lines of defence in the effective management of risk. These are:

i. Day-to Day Operations Management:

As staff carry out their day-to-day activities we should all be aware of the risks related to our jobs. We are all responsible for ensuring these risks are identified and managed, or escalated to the correct level should they be significant. Managers, project and process owners must all ensure that appropriate controls are in place to ensure the risks are managed in line with this Strategy, and that they are designed into the systems and processes under their areas of responsibility.

ii. Risk Management & Compliance Functions

Functions involved in the oversight and monitoring of the first line of defence are seen as the second line in the management of risk. The functions ensure compliance with policy and procedure, provide training and advice and regularly assess risk management arrangements within the organisation. Examples of these within Invest NI include:

- Risk Management Team
- Financial Management Team
- Business Solutions Development & Compliance Team
- Human Resources
- Procurement
- Information Management & Governance

However, many other structures throughout the organisation fit into this category, such as senior management, Executive Leadership Team and the Invest NI Board and its Committees.

iii. Internal Audit

The Internal Audit function provides independent opinion on the overall adequacy and effectiveness of the organisation’s framework of governance, risk management and internal control to the Accounting Officer. As the third line of defence they review the adequacy of both lines one and two.

3.2 Roles and Responsibilities

Accounting Officer:

- Retains ultimate responsibility for the organisation's system of internal control and ensures that an effective risk management process is in place and is regularly reviewed;
- Provides clear direction to staff;
- Establishes, promotes and embeds an organisational risk culture;
- Allocates an officer as the Business Risk Officer (Risk Manager) to manage the organisation's risk management process; and
- Reports to the Board and the Audit & Risk Committee.

Invest NI Board:

- Endorses the risk management strategy/policies;
- Establishes and oversees risk management procedures;
- Ensures appropriate monitoring and management of significant risks by management;
- Challenges risk management to ensure that all key risks have been identified; and
- Is aware of any instances where risks have not been adequately managed.

Invest NI Audit & Risk Committee:

- Regularly reviews the Control Environment;
- Ensures that risk management is a standing item on the Audit & Risk Committee agenda;
- Reports to the Board on the effectiveness of the system of internal control and alerts the Board members to any emerging issues;
- Takes responsibility for the oversight of the risk management process; and
- Reviews risk registers to provide challenge and advice.

ELT:

- Acts on behalf of the Board and will:
    - Determine the organisation's approach to risk management;
    - Implement policies on risk management and internal control;
    - Discuss and approve issues that significantly affect the organisation's risk profile or exposure;
    - Continually monitor the identification and management of emerging and significant risks and ensure that actions to remedy control weakness are implemented;
    - Report changes in risk assessment to the Board on an exception basis;
    - Annually review the organisation's approach to risk management and approve changes or improvements to key elements of its processes and procedures; and
    - Report to the Audit & Risk Committee and to the Board on risk management matters.

- Initiates reports, including exception reports, as appropriate to keep the Invest NI Board and committees fully informed of risk management progress;
- Prepare and update (quarterly) Risk Registers for their Groups and input into the Corporate Risk Register for review by the Chief Executive and Audit & Risk Committee;
- Allocates a Responsible Officer to maintain, update and monitor the Risk Register. To co-ordinate with the Risk Manager and report to the Executive Director progress on additional actions;
- Ensures that risk management is a standing agenda item on each Group's Monthly Management Meeting, with all discussion and decisions minuted for audit purposes;
- Determines when a trigger point has been reached for risks to be considered for escalation to the Corporate Risk Register, based on risk appetite and guidance provided within this policy; and
- Provides a quarterly Stewardship/Assurance Statement to the Chief Executive expressing satisfaction that appropriate management controls are in place supported by a comprehensive risk management process.

All management:

- Ensure that all significant areas of the business under their stewardship are subject to risk assessment and risk management processes;
- Ensure that all key programmes and projects, new initiatives and business areas, and areas of significant change are risk assessed and managed as appropriate, including Privacy Impact Assessments where applicable; and
- Ensure that all corporate and business objectives, systems and operations are reviewed quarterly.

Risk Owner:

- Identifies and assesses individual risks;
- Decides whether a risk is sufficiently serious to be escalated to the next level of the organisation;
- Ensure that actions to treat or control the risk are carried out and informs the Risk Manager of any consequent updates to the risk register;
- Reviews the risk rating and the necessity to keep the risk on the register.

Risk Management Team:

- Identifies and records emerging risks on emerging risk register;
- Maintains the risk registers under the direction of risk owners and updates or amends the risk register as necessary;
- Regularly reviews the content of risk registers with a view to ensure that risk actions are being completed and that all details on the risk register are correct;
- Provide support and challenge; and

- Keeps up to date and abreast of developments in risk assessment methodologies and advises the Invest NI Board and Executive Directors of their possible introduction within Invest NI.

Data Protection Officer:

- Provide advice and guidance on privacy risks in relation to compliance with the General Data Protection Regulation (GDPR);
- Provide advice and guidance on completion of a Data Protection Impact Assessment (DPIA);
- Review of DPIAs to confirm whether its conclusions are in compliance with GDPR.

Staff:

- Carry out risk mitigation actions identified and delegated by the risk owners;
- Maintain awareness of the organisation's risk management strategy/policy and the key risks faced by the organisation; and
- Ensure that duties relating to controls are fully discharged.

Internal Audit:

- Provides technical support and guidance on new initiatives in risk management; and
- Audits and reports on the effectiveness of the risk management process

While the roles above have particular responsibilities in the management of risk across the organisation it should be stressed again that *everyone* is responsible and accountable for ensuring risks are recognised, recorded and mitigated adequately. This will foster the integration of risk management into the culture of the organisation.

3.3 Communication

The Risk Management Strategy and Policy will be published on the Invest NI intranet for access by all members of staff. Notification of the publication will be communicated through the regular staff newsletter email ('Newsweekly') and online awareness sessions will also be provided for completion by all staff. A single/two page flyer will also be produced for display in Invest NI facilities as required. A dedicated Risk Management area will also be developed on the Invest NI intranet for the publication and sharing of other relevant materials, guidance or information that may be useful to staff (case studies, best practice, government guidance etc.).

To ensure an efficient and effective system of risk management is provided within Invest NI, the methods of risk recording, monitoring, reporting and communication will also be reviewed on a regular basis with a view to utilising current or future technology in continually improving arrangements.

3.4 Training

First Time/Induction Training

Via the Learning & Development team, all employees will be provided with an online risk awareness training module and, where appropriate, any member of staff who will need to engage with the formal risk management process will be invited to formal risk management training by the Risk Manager.

Refresher Training

Refresher training workshops for staff with functional responsibilities will be run as appropriate.

Annual refresher training, in the form of an e-learning package will be mandatory for all staff with regards to risk awareness training.

Recognition

Management in Invest NI will be supportive of those actively seeking to understand and manage risks as they arise. This can be recognised through the internal performance management and recognition processes where appropriate.

3.5 Evaluation

It is the aim of Invest NI to continuously improve risk management arrangements so they will be reviewed for effectiveness at least annually. This will be done by the Audit & Risk Committee as part of its Annual Report and by Internal Audit as part of the rolling programme of audits.

4.0 RISK MANAGEMENT PROCESS

4.1 Identifying Risks

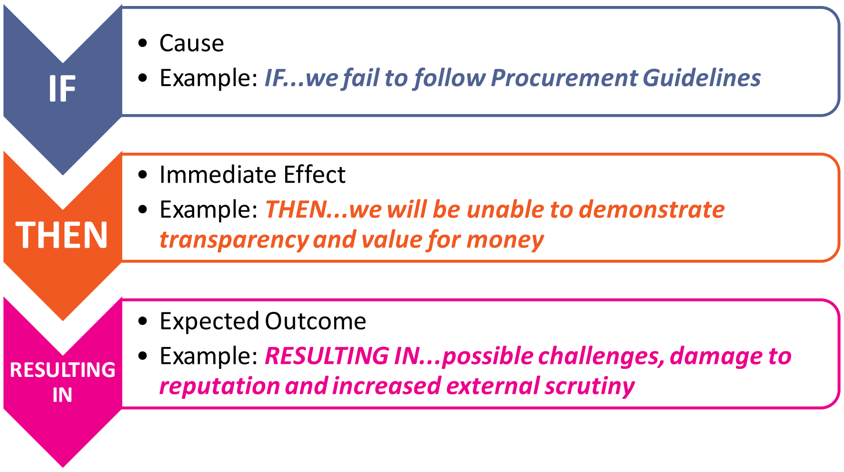
Risk identification is the process of identifying risks which may impact on the organisation's ability to achieve its objectives. The aim is to identify what, when, where, why and how events could prevent, degrade, delay or enhance achievement of objectives. Risk categories include:

- Financial/Compliance e.g. failure to meet legislative standards, financial loss or fraud;
- Operational e.g. risk/opportunities associated with a new client;
- Reputational e.g. the organisation receiving negative media coverage, Northern Ireland being reflected poorly in international arenas; and
- Infrastructure e.g. IT systems crashing or losing water/heating facilities.

This is a continuous process in which new risks are identified, amended and updated and/or eliminated when no longer valid or have been fully addressed. Risks can be identified at any time and must be reported to Divisional or Executive Directors so they can be recorded, assessed and acted upon. It is good practice for a risk assessment to be conducted at the outset of any new project, policy change or initiative so that risks can be identified, assessed and managed through the processes outlined in this Risk Management Policy.

4.2 Defining a Risk

When a risk has been identified is it important that it is clearly defined in terms of the cause, the direct effect and, should the risk be realised (actually happen), the outcome that could be expected. Therefore all risks being recorded may take the form of **IF** (cause), **THEN** (immediate effect) and **RESULTING IN** (expected outcome).



- Cause
- Example: *IF...we fail to follow Procurement Guidelines*

- Immediate Effect
- Example: *THEN...we will be unable to demonstrate transparency and value for money*

- Expected Outcome
- Example: *RESULTING IN...possible challenges, damage to reputation and increased external scrutiny*

Existing risk registers that do not have risks defined in this format need not be changed but any new risks added to them should take this guidance into consideration.

4.3 Privacy Risks

All projects being undertaken that involve collecting and/or using personal information give rise to risks related to privacy issues and data protection.

Privacy risks not only relate to the security of personal data but also refer to the protection of privacy rights and freedoms of individuals i.e. compliance with the General Data Protection Regulation Principles [lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality] and Rights [transparency; information access; rectification, erasure, restriction and data portability; and the right to object].

To enable Invest NI to address these concerns every project that involves collecting and/or using personal information must undergo a Data Protection Impact Assessment (DPIA) Screening exercise, to determine if a full assessment is required. The Data Protection Officer (DPO) should be consulted when completing this exercise.

Further information can be found in the Data Protection Impact Assessment Guidance and Procedural Manual available on the intranet. All DPIAs should be reviewed by the DPO to confirm whether its conclusions are in compliance with GDPR. For consistency, DPIAs should follow the guidance contained within this Risk Management Strategy & Policy in terms of identifying and assessing risks, and identified risks should be included in project risk registers where possible. Where project risk registers are not available privacy risks should be recorded in a specific privacy risk register.

4.4 Gateway Review Risk Potential Assessments

Some programmes and projects being undertaken within Invest NI may need to engage with the Gateway Review process, administered by the Department of Finance's Centre of Excellence for Programme and Project Management (CoE PPM). As such, the first step of ***any*** project or Programme of work should be the completion of a Risk Potential Assessment (RPA), which will inform whether the Gateway process is applicable. More information, along with a template for the completion of an RPA, can be found at https://www.finance-ni.gov.uk/publications/gateway-risk-potential-assessment.

4.5 Risk Workshops

To facilitate the holistic review of organisational risk and ensure that identified risks do not stagnate, workshops will be held, at least annually, to assess the risk profile of the organisation. While these will primarily involve members of the Invest NI Board and Executive Leadership Team, it is anticipated that all leaders throughout the organisation should hold similar events to inform their own planning processes. The outcome of these risk workshops will be included within the Corporate Risk Register and cascaded to Groups as necessary.

4.6 Horizon Scanning

The risk workshops should also allow opportunity for what is known as horizon scanning. This is the practice of monitoring the external and internal business environments, and identifying and tracking any changes in those environments that could potentially impact Invest NI. These risks are captured on the Emerging Risk Register, which operates in support of the Corporate Risk Register and is reviewed by the Audit & Risk Committee twice yearly.

4.7 Assessing Risks

Risk assessment is undertaken considering:

- The likelihood of the risk materialising (from a scale of 1, being low to 5, being high) and;
- The impact that the risk would have on the business given that the risk has occurred (from a scale again of 5 (high) to 1 (low)).

For all risks this should be applied in 2 scenarios:

1. If the risk was to be realised (actually happen) without anything in place to lessen the damage that could occur – this is known as the ***inherent risk***
2. If the risk was to be realised (actually happen) taking into consideration anything that has already been done to limit the damage that could occur – this is known as the ***residual*** or ***mitigated risk***

How likely is it to happen?

What damage will occur if it does happen?

How significant is the combination of both?

Likelihood
Impact
Risk Rating
(Consequence)

Guidance on the scales for assigning likelihood and impact, and the consequence matrix are shown below:

Impact Assessment

Impact Type	**I1**	**I2**	**I3**	**I4**	**I5**
Guidance on potential Impact categories and severity of Impact					
Project Delivery	If risk materialises, there would be very little impact to the successful delivery of the project eg minor delay (days) or additional cost (£1,000's) and/or low impact to the anticipated economic and/or commercial benefits of the project (80-100% still expected).	If the risk materialises, there would be low impact to the successful delivery of the project eg minor delay (1-2 weeks) or additional costs (£10,000's) with the majority (50-80%) of economic benefit still expected to be delivered, breach of legal/regulatory requirements but minimal penalty, limited local media coverage.	If the risk materializes, there would be medium impact to the project, with less than half (20-50%) of the economic benefit expected to be delivered, moderate additional cost (£100,000's), delay to the completion of works in the region of 2-4 weeks, breach of legal/regulatory requirements resulting in investigation/review and potentially legal action.	If risk materializes, there would be a significant impact on the project eg legal action, significant (months) delay to the works, additional costs (£500,000-£1,000,000), sustained national and limited international media coverage, little (<20%) expected economic benefit.	If risk materializes, there would be a serious impact on the project eg major litigation, contractor default, land being unusable, significant additional costs (£millions), no economic benefit, sustained national and international media coverage.
Safety/Harm	Minor Injuries	Major Injury.	Major Injuries.	Single Fatality.	Multi Fatality.
Reputational Impact	Customer complaints increase.	Customer complaints increase.	Limited local media coverage.	Limited national media coverage.	Sustained national and limited international media coverage.
Legal & Regulatory e.g. Employment, Equality, State Aid, Procurement	Breach of Policy, but an isolated incident and not indicative of systemic failure.	Breach of legal duty, regulatory or contractual obligations. Regulator requiring corrective action or contractual obligations, or risk of legal action and may result in minimal penalty.	Regulatory, legal duty or contractual breach with costs to Invest NI and increased scrutiny from the Regulator (eg State Aid/ERDF) or legal action from the customer.	Regulatory censure or legal action. Significant breach of contract or rules. Action taken against individual members of senior management or regulatory enforcement action.	Public regulatory fines and censure, major litigation and potential for prison sentences for senior management.

Likelihood Matrix

Likelihood Classification	Guide	Examples
L5	Almost Certain	This event is already occurring or is expected to occur/recur in the next 12 months, possibly frequently (>75% chance of occurrence)
L4	Likely	This event has not yet happened, but it is probable that it will occur in the next 18 months (50-75% chance of occurrence)
L3	Possible	This event has not yet happened, but it is possible it may do so in the next 24 months (35-50% chance of occurrence)
L2	Unlikely	This event has not yet happened, but it is possible it may do so in the next 36 months (25-35% chance of occurrence)
L1	Very unlikely	This event is unlikely to happen (<25% chance of occurrence)

Consequence Matrix

When the Likelihood and Impact are combined an overall score is allocated based on the matrix below. This score is then used to identify how significant the risk is and determine what priority it should be given.

Impact **Likelihood**	***I1***	***I2***	***I3***	***I4***	***I5***
L5	**5**	**10**	**15**	**20**	**25**
L4	**4**	**8**	**12**	**16**	**20**
L3	**3**	**6**	**9**	**12**	**15**
L2	**2**	**4**	**6**	**8**	**10**
L1	**1**	**2**	**3**	**4**	**5**

Risk Ratings

Colour	Risk Rating	Risk Score
Red	**Very High**	**>15**
Amber	**High**	**10-15**
Yellow	**Medium**	**5-9**
Green	**Low**	**<5**

It is important that staff should avoid rushing through the risk process or ‘cutting corners’. This could lead to serious risks not being identified or adequately addressed.

4.8 Risk Appetite – Definitions

Risk Appetite is the amount of risk that an organisation is prepared to accept, tolerate or be exposed to at any point in time

The following definitions of categories of risk appetite reflect those commonly found in best practice guidance on risk management including that issued by HM Treasury:

Averse	**Avoidance** of risk and uncertainty is a key organisational objective.
Minimalist	Preference for **ultra-safe** business delivery options that have a low degree of inherent risk and only have a potential for limited reward.
Cautious	Preference for **safe** delivery options that have a low degree of inherent risk and may only have limited potential for reward.
Open	Willing to consider all potential delivery options and choose the one that is **most likely to result in successful delivery** while also providing an acceptable level of reward.
Hungry	**Eager to be innovative** and to choose options offering potentially higher business rewards.

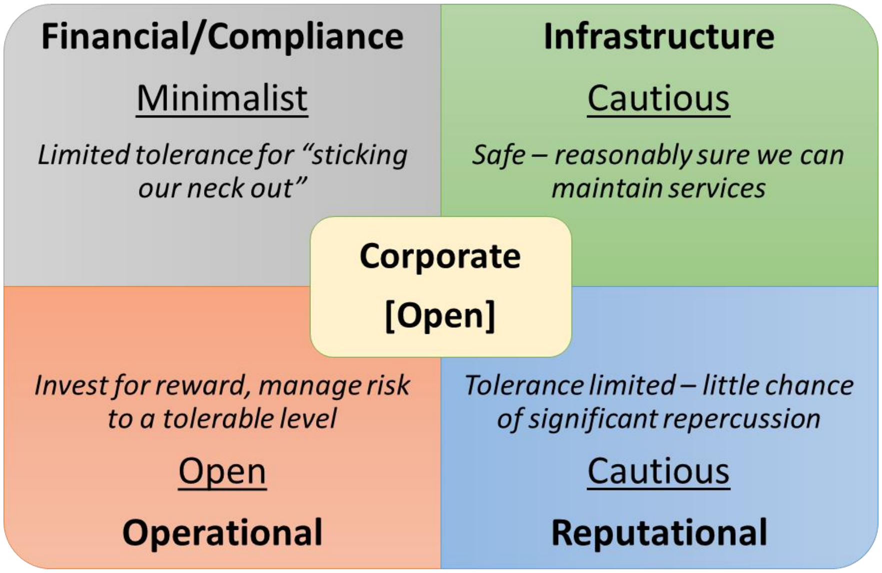
A matrix of “example behaviours” for each category of risk, and for each level of risk appetite is provided later in this section. As with the definitions above, the example behaviours are based on best practice guidance, and in some cases the distinction between the various appetites and the associated example behaviours is somewhat limited. Without reference to the example behaviours, there is arguably a tendency to misinterpret the various appetites – e.g. an “open” risk appetite for operational matters refers to the responsibility for non-critical decisions being devolved, <u>it does not mean that Invest NI policies and procedures relating to those decisions can be ignored</u>.

4.9 Risk appetite Framework

Invest NI's risk appetite is not necessarily static; in particular the Board and Executive Leadership Team will have freedom to vary the amount of risk which it is prepared to take depending on the circumstances at the time. The model below sets out these concepts in more detail.

Risk Appetite is set at Corporate level which, in turn, forms the basis for cascading levels of tolerance down throughout the organisation to divisional level.

The diagram below depicts the 4 quadrants within which risk management operates and the risk appetites agreed for each.



Financial/Compliance

Minimalist

Limited tolerance for "sticking our neck out"

Infrastructure

Cautious

Safe – reasonably sure we can maintain services

Corporate

[Open]

Invest for reward, manage risk to a tolerable level

Open

Operational

Tolerance limited – little chance of significant repercussion

Cautious

Reputational

Example behaviours for the proposed risk appetite framework are set out below:

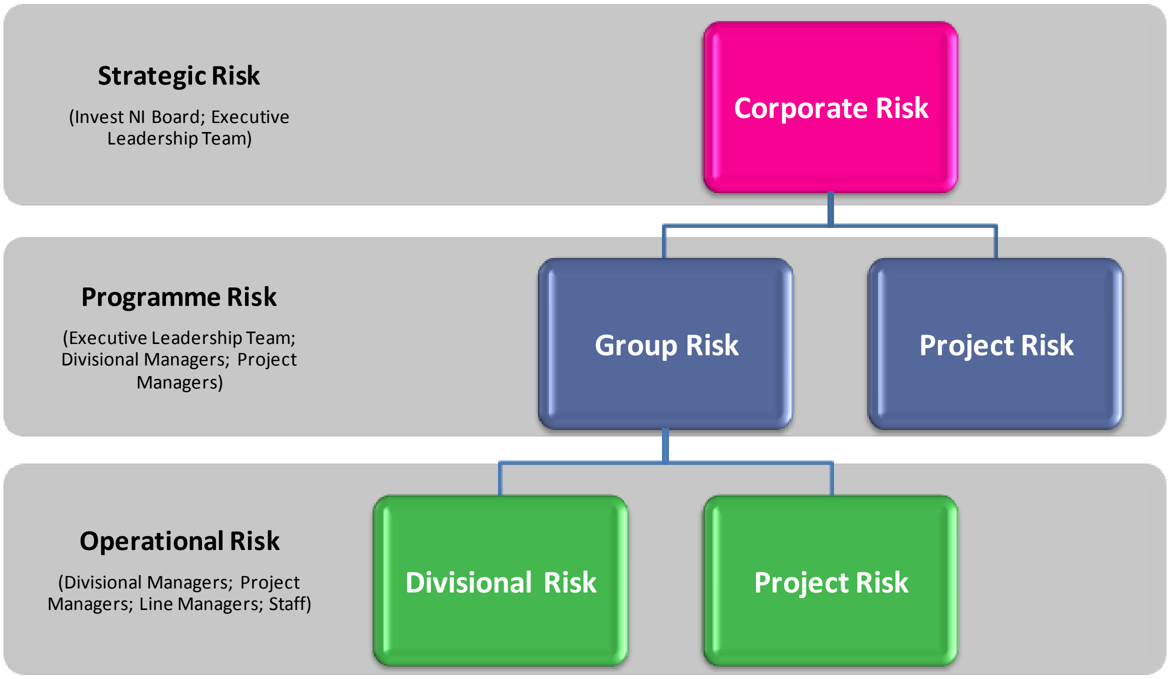
Financial/compliance – minimalist	Infrastructure – cautious
Only prepared to accept the possibility of very limited financial loss if essential.	Prepared to accept limited repercussion.
VfM the primary concern but willing to consider the benefits.	Want to be reasonably sure we can maintain services.
Limited tolerance for sticking our neck out. Want to be reasonably sure we would win any challenge.	
Operational – open	**Reputational – cautious**
Prepared to invest for reward and minimise the possibility of loss by managing the risks to a tolerable level.	Minimal tolerance for any decisions that could lead to scrutiny of the organisation. Tolerance limited to those events where there is little chance of any significant repercussion should there be a failure.
Innovation supported with demonstration of commensurate control	
Responsibility for non-critical decisions may be devolved.	

The risk appetite framework reflects where the organisation wants to be, rather than where it is perceived to be at present. It could be argued that in adopting a risk averse position, risk may be "over-managed" whereas a more cautious appetite may be more appropriate. Again, it is emphasised that a more cautious, or open, risk appetite does not translate into a carte blanche to breach or ignore the organisation's established policies, procedures and guidelines.

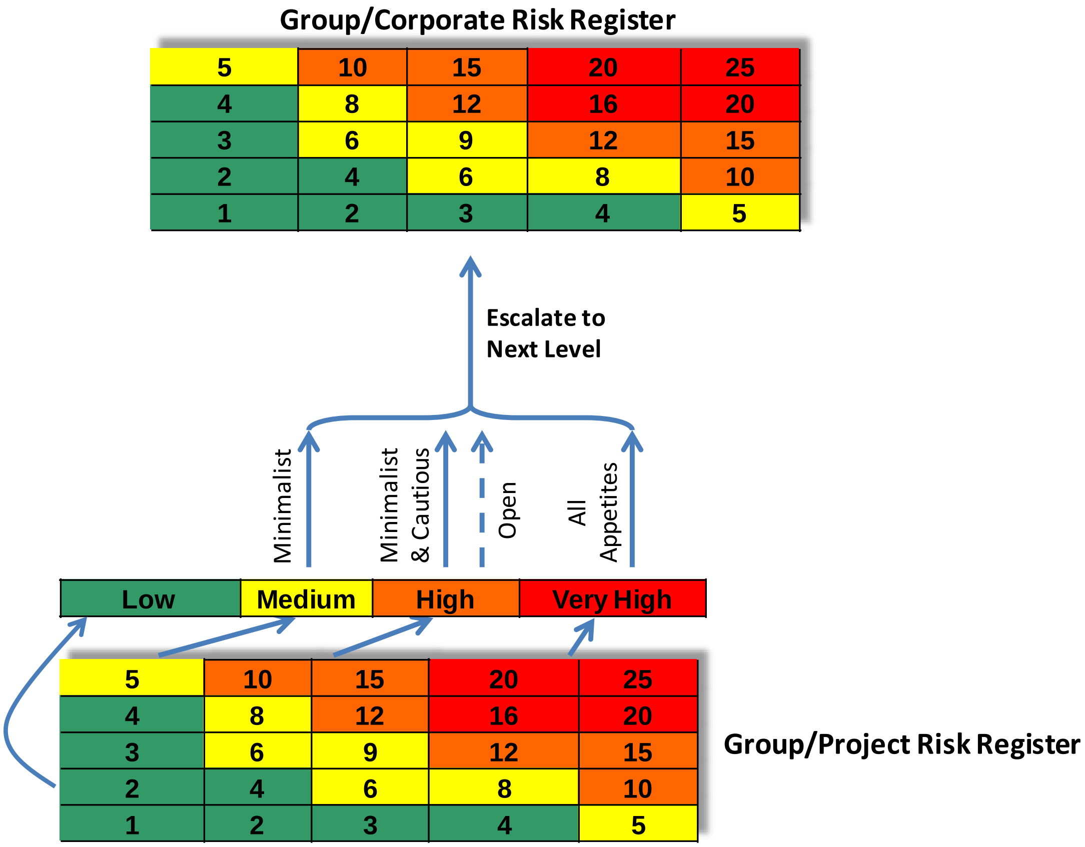
The day-to-day activity of Invest NI will fall within the "**operational**" segment where an "open" appetite is proposed. In seeking to meet its objectives, Invest NI should position itself as an organisation that actively seeks to develop and support projects that will benefit the economy – if this is to be achieved, the organisation should adopt a proactive approach to operational risk, with a focus on maximising opportunities and a "no surprises" risk culture, rather than adopting a reactive approach to the management of threats. The management of operational risk should, in the main, be dealt with through existing operating procedures and approval processes. However, a limited number of projects may, by virtue of their size and/or nature, require more robust consideration of risk.

The identification of such projects should be determined by the project team, through consideration of a range of quantitative and qualitative parameters such as: the scale of Invest NI's commitment (e.g. more than £6m); the cost per job; the level of proposed job creation; the nature of the assistance (e.g. upfront payment of grant assistance); the nature of the project (i.e. if it is potentially novel or contentious); the stage of development of the company (e.g. early stage start-ups); and legal or compliance issues. It should be noted than in many cases, the increased qualitative parameters involve the project being approved at a higher delegated authority and more closely monitored, which form part of the mitigating actions to manage the risk.

For projects classified as "high risk", a project specific risk register should be established and monitored on a regular basis by the project team, with risk escalated "up the line" if/when risks associated with the project approach, or exceed, acceptable boundaries. In the case of Invest NI this should equate to escalations from project/divisional risk registers to their Group risk register and, in turn, from Group Risk Registers to the Corporate Risk Register (see figure below).


Strategic Risk
(Invest NI Board; Executive Leadership Team)
Corporate Risk
Programme Risk
(Executive Leadership Team; Divisional Managers; Project Managers)
Group Risk
Project Risk
Operational Risk
(Divisional Managers; Project Managers; Line Managers; Staff)
Divisional Risk
Project Risk

To facilitate this, a scheme of escalation is outlined on the next few pages, based on the risk appetites already defined for the organisation. While risks escalated to a higher level risk register can be included verbatim, similar risks being experienced by other functions can be rolled into one overarching risk as necessary. These risks are then re-assessed to identify likelihood and impact in the context of the new level of escalation.



Group/Corporate Risk Register

5	10	15	20	25
4	8	12	16	20
3	6	9	12	15
2	4	6	8	10
1	2	3	4	5

Group/Project Risk Register

5	10	15	20	25
4	8	12	16	20
3	6	9	12	15
2	4	6	8	10
1	2	3	4	5

Guidance on the acceptable levels of risk for each risk appetite are shown below, with some simple example scenarios provided in Annex B. Whereas the appetites below are those defined by Invest NI for each category of risk it is recognised that these may not always be suitable. Officers responsible for the management of risk within their departments can define risk appetites based on their own circumstances, but should use those below as a starting point.

4.10 Risk Appetite/Escalation

Risk Category	Risk Appetite	Description	Acceptable Range (up to and including)	Escalation
Corporate	Open	Willing to accept a reasonable amount of risk based on perceived rewards	**High**	• Executive Director to decide if risks assessed as High should be escalated to Board level
Financial/ Compliance/ Governance	Minimalist	Preference for ultra-safe options and low inherent risk	**Low**	• Risks greater than Low to be included in Corporate Risk Register
Infrastructure	Cautious	Safe – reasonably sure we can maintain services	**Medium**	• Risks above Medium to be included in Corporate Risk Register
Reputational	Cautious	Safe options with low inherent risk. Tolerance limited to little chance of any significant repercussions	**Medium**	• Risks above Medium to be included in Corporate Risk Register
Operational	Open	Invest for reward, manage risk to a tolerable level, choose the option most likely to result in successful delivery	**High**	• Executive Director to decide if risks assessed as High should be included in Corporate Risk Register
	Hungry	Invest for the best possible reward and accept the possibility of financial loss without any guarantee of return on investment	**Very High**	• Regardless of the risk appetite, INI ELT should be made aware of any Group Risks assessed as red and advised immediately of any early warning signals that the risk may be realised. • Contingency plans should also be developed and tested. • ***ELT to agree if the risk is to be included in the Corporate Risk Register***

Risk Appetite	***Averse***	***Minimalist***	***Cautious***	***Open***	***Hungry***
Risk Rating	***Very Low***	***Low***	***Medium***	***High***	***Very High***
Corporate	▨			■	
Financial	▨	■			
Infrastructure	▨		■		
Reputational	▨		■		
Operational	▨			■	

By recognising, and seeking to manage such risks “up front”, the organisation can focus on maximising opportunity in an informed manner whilst adopting a proactive approach to the management of associated risks at the appropriate level within the organisation.

It is accepted that the nature of some risks mean they are likely to have a high residual rating even after the controls are in place. If the senior officer responsible for the relevant risk register is satisfied that all reasonable steps have been taken to manage the risk and is content to accept a particular risk at a higher than normal rating i.e. have a greater appetite for that risk, then the manager can direct that the risk be managed via its existing risk register despite it being outside the normal risk appetite. All Group risks with a ‘Very High’ rating must be presented to ELT for discussion and decision as to whether they should be escalated to Corporate level. All Corporate risks with a ‘Very High’ rating must be escalated to the Audit & Risk Committee for discussion and communicated to the Accountability & Casework Team in the Department for the Economy (DfE) for discussion at the Departmental Board and Departmental Audit & Risk Assurance Committee.

However, it is important that risks included in registers are scored realistically. This will ensure the integrity of the process and that risks are escalated only when they need to be, with the aim being that all risks are managed at the correct level and managers are empowered to implement controls within their own areas of responsibility.

The process for managing risks with a ‘High’ or ‘Very High’ rating is, in theory, the same as for all risks; i.e., the risk is identified and assessed, with mitigation or control measures put in place and progress monitored and reviewed regularly. However, it is acknowledged that, in practice, risks in the ‘High’ or ‘Very High’ categories are subject to closer scrutiny and additional control measures or mitigating actions may need to be put in place in order to manage the risk to an acceptable level.

4.11 Risk Appetite – Example Behaviours

Category of Risk	Averse	Minimalist	Cautious	Open	Hungry
Financial (and Compliance)	Avoidance / limited financial loss is a key objective.	Only prepared to accept the possibility of very limited financial loss if essential.	Prepared to accept the possibility of some limited financial loss.	Prepared to invest for reward and minimise the possibility of financial loss by managing the risks to a tolerable level.	Prepared to invest for the best possible reward and accept the possibility of financial loss (although controls may be in place).
	Only willing to accept the low cost option.	VfM is the primary concern.	VfM still the primary concern but willing to also consider the benefits.	Value and benefits considered (not just cheapest price).	Resources allocated without firm guarantee of return (Investment capital approach).
	Resources withdrawn from non-essential activities.		Resources generally restricted to core operational targets.	Resources allocated in order to capitalise on potential opportunities.	Chances of losing are high and consequences serious but a win would be seen as a great coup.
	Play safe. Avoid anything which could be challenged, even unsuccessfully.	Want to be very sure we would win any challenge.	Limited tolerance for sticking our neck out. Want to be reasonably sure we would win any challenge.	Challenge will be problematic but we are likely to win it and the gain will outweigh the adverse consequences.	
Infrastructure	Play safe. Avoid anything which could be challenged, even unsuccessfully.	Want to be very sure we would win any challenge.	Limited tolerance for sticking our neck out. Want to be reasonably sure we would win any challenge.	Challenge will be problematic but we are likely to win it and the gain will outweigh the adverse consequences.	Chances of losing are high and consequences serious but a win would be seen as a great coup.

Category of Risk	Averse	Minimalist	Cautious	Open	Hungry
Operational	Defensive approach to objectives – aim to maintain or protect rather than to create or innovate. Priority for tight management controls and oversight with limited devolved decision making authority. General avoidance of systems/ technology developments.	Innovations always avoided unless essential. Decision making authority held by senior management. Only essential systems/ technology developments to protect current operations.	Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior management. Systems/ technology developments limited to improvements to protection of current operations.	Innovations supported with demonstration of commensurate improvements in management control. Responsibility for non-critical decisions may be devolved. Systems/ technology developments considered to enable operational delivery.	Innovation pursued – desire to "break the mould" and challenge current working practices. High level of devolved authority – management by trust rather than tight control. New technologies viewed as a key enabler of operational delivery.
Reputational	Minimal tolerance for any decisions that could lead to scrutiny of the Department or Agency. Tolerance limited to those events where there is little chance of any significant repercussion should there be a failure.	Tolerance for risk taking limited to those events where there is no chance of any significant repercussion for the Department or the Agency.	Tolerance for risk taking is limited to those events where there is little chance of any significant repercussion for the Department or Agency should there be a failure.	Appetite to take decisions with potential to expose the Department or Agency to additional scrutiny but only where appropriate steps have been taken to minimise any exposure.	Appetite to take decisions that are likely to bring scrutiny of the Department or Agency but where potential benefits outweigh the risks.

4.12 Risk Population & Risk Registers

As mentioned throughout this document, risks faced by projects, divisions, groups and the organisation will be captured in a series of Risk Registers. Due to the variety of situations in which risk registers are used there is no single template for how they should look, but the contents and practicalities of how they are used should be in line with the guidance provided in this policy.

With that in mind all risk registers should, as a bare minimum, include:

Field	Description
Risk Category	The type of risk identified e.g. Financial/Compliance, Infrastructure, Reputational, Operational
Risk	The definition of the risk using the 'IF', 'THEN', 'RESULTING IN' format
Description	Any further details to needed to help clarify the risk
Corporate Objective	This should detail the corporate objective (or objectives) that would be most affected should the risk materialise
Risk Appetite	The appetite assigned to this specific risk. Where possible this should be in line with the guidance provided in Section X of this document by risk category.
Unmitigated Risk Analysis	This should clearly show the likelihood, impact and consequence score for each risk, before any controls have been put in place.
Controls/Mitigations	Details of the actions already taken to mitigate the risk identified. **Note:** this should not include proposed controls that are still to be implemented
Residual (Mitigated) Risk analysis	This should clearly show the likelihood, impact and consequence score for each risk, taking into account the controls already in place.
Response Notes/Action Plan	This should include any notes on ongoing control activity, including details for further control actions. Further actions should have an owner identified and expected completion dates.
Risk Owner	This is the named individual who has overall responsibility for the mitigation and monitoring of the risk identified
Previous Score	This should record the Residual Consequence score from the last time the risk was reviewed
Date of Last Review	The date the risk was last reviewed and updated
Date of Next Review	The date the risk is next due to be reviewed and updated

Any other fields felt necessary for the effective operation of the risk register may be added but it is also important to avoid over-engineering the process. Risk management is about proportionality so the extent of assessment required will be dependent upon the level of risk. Registers should not include too many risks, but should focus on the key risks to the successful achievement of objectives. Best practice indicates that attempting to manage any more than 20 risks at any one time is unwieldy and counterproductive, and suggests that risks are being “over-managed”.

The current Corporate Risk Register can be obtained by contacting the Invest NI Risk Manager.

Risk Register Audit Trail

To ensure an audit trail is maintained for all changes to entries in risk registers a number of mechanisms should be used to identify amendments:

1. Additions/amendments should be highlighted in red
2. Deletions should be highlighted in blue
3. Comments or updates at each review should be captured in a new column

It is therefore suggested that where practical, a ‘Tracked’ version of the risk register should be held, showing all amendments, with a ‘Final’ version used for reporting purposes (without colour coding).

The Audit & Risk Committee should be provided with a summary of the Corporate Risk Register Audit Trail each time the Register is reviewed and updated. In the event that the Corporate Risk Register is requested by a body outside Invest NI (e.g. Northern Ireland Audit Office), the Audit & Risk Committee will be provided with a summary of additions / deletions and movement around the ‘Very High’ rating before the Register is released to that outside body.

Removal of Risk from Risk Register

It is the nature of risk that it can increase or decrease in significance over time, so it is important that risk can not only be added to risk registers but also removed. This reduction in risk can result from a change in the internal or external environment, or due to the controls put in place to mitigate it. There is also a need to recognise that with the implementation of control mechanisms, the law of diminishing returns can apply, effectively meaning that further mitigation of the risk ceases to be feasible or, indeed, economically viable.

One or more of the following criteria can therefore be applied to the decision to remove risks from risk registers:

1. Risk has been within the acceptable rating for the risk appetite for the last 2 risk reviews
2. Risk consequence score has remained unchanged for the last 2 reviews and Register Owner deems the risk to be at an acceptable level
3. No further mitigations are planned or have been implemented for the last 2 review periods and Register Owner deems the risk to be at an acceptable level

All risks removed from the register should be kept in a ‘risk log’ for audit purposes, along with the rationale for their removal. Should the risk return, a new entry should be made in the register.

4.13 Risk Mitigation

If a risk is not being managed to an acceptable level, additional controls or mitigating actions may need to be put in place. These additional actions or mitigation plans can be split into various options:

Category	Definition
Transfer the risk	This includes paying a third party to take the risk or by conventional insurance.
Tolerate the risk	The ability to do anything about some risks may be limited, the risk may be considered to be low priority or the cost of taking action may be disproportionate to the potential benefit gained.
Terminate the risk	Some risks will only be treatable or containable to acceptable levels by terminating the activity or designing/simplifying a business process to avoid or reduce the risk.
Treat the risk	The majority of risks will belong in this category and the purpose is to contain the risk within an acceptable level.

4.14 Monitoring & Testing

Risk management should be a dynamic process. New risks will be identified, some terminated, contingency plans and countermeasures will need to be updated in response to changing internal and external events, and assessment of likelihood and impact will also need to be reviewed, particularly in the light of management actions.

Monitoring of risks, therefore, should be performed by all managers within Groups and Divisions on a continual basis, and at least quarterly, through a review of risk registers. It is also important to ensure that mitigations or controls already in place are tested. This provides confidence that they do in fact reduce the level of the risk as intended.

Ideally, where possible, mitigations or controls should be tested and validated in such a way as to provide proof that the results are as intended. While this may not be possible in the majority of cases the possibility of formal verification should be investigated. An example of this could be external certification/accreditation against a recognised framework, although internal scenario testing or 'dry runs' could also be utilized.

4.15 Reporting

Risk reporting is fundamental to risk management. Reporting provides assurances to management that risks are being regularly reviewed and effectively managed. Below is a table of the different levels of reporting associated with the risk management process.

Reported To	Format	Timescale
NI Executive	Governance Statement	Annual
Permanent Secretary	Assurance Statement	6-Monthly
Invest NI Board	Corporate Risk Register	Annually (or as necessary for escalations)
Invest NI Audit & Risk Committee	Corporate Risk Register	Quarterly (or as necessary for escalations)
Accounting Officer	Assurance Statement	Quarterly
Executive Leadership Team	Corporate & Group Risk Registers	Quarterly
Project/Programme Managers	Programme/Project Risk Registers	Regular Programme/Project Reviews

As can be seen the regular completion of risk registers (at least quarterly) facilitates the population of Stewardship Statements and ultimately Assurance and Governance Statements provided to the Permanent Secretary and NI Executive.

The Executive Leadership Team (ELT) and Directors should on a quarterly basis, as part of their Group Meeting structure, formally review and update the risk register with their management team ***and ensure a documented record of the discussion is maintained***. When reviewing and assessing the risk register the following should be considered:

- Review the risks and how they were identified, evaluated and managed.
- Evaluate whether there are any new risks.
- Evaluate whether any existing risks are no longer relevant.
- Evaluate whether the risks previously identified are still acceptable.
- Review the effectiveness of the internal control system in managing the significant risks and whether amendments need to be made to control systems.
- Assess whether any current or possible future failures or weaknesses exist in the system of internal control and the promptness of corrective actions in response to their identification.
- Assess if control strategies need to be changed.
- Ascertain if findings require a more extensive monitoring process; and
- Evaluate the response time to change.

Risk information and assessments will be recorded and stored using existing resources within Invest NI IT infrastructure (e.g. MS Office applications) and, where necessary, manual filing systems. This will be reviewed on an ongoing basis and, based on need, the introduction of risk management software may be considered.

At present all risk registers are maintained in Microsoft Excel spreadsheet format.

Once updated, risk registers should be forwarded to the Performance, Compliance and Co-ordination Division.

4.16 Stewardship Statements

Executive Directors and/or Directors must complete a Stewardship Statement. This should be completed at both Group and Divisional levels. A template is attached at Annex C. The purpose of the stewardship statements is to ensure that ownership and accountability are brought to the risk management process. Completed Statements should be returned along with the Risk Register to the Performance, Compliance and Co-ordination Division.

4.17 Timescales

Corporate and Group Risk Registers are reviewed quarterly, with the Corporate Risk Register to be approved by ELT at the next available meeting following the resolution of any queries as a result of challenge by the Risk Management Team. This will ensure a timely and continual review of outstanding risks in line with best practice.

5.0 INFORMATION RISK

Invest NI is certified to the International Standard ISO27001 for Information Security. The Invest NI information security management system (ISMS) preserves the confidentiality, integrity and availability of organisational information by applying a risk management process that gives confidence that risks are adequately managed.

The guidance and methodology provided in this Policy is applicable to the management of information risk throughout Invest NI. There is a specific Information Security Risk Register, operating alongside the Corporate and Group risk registers, that is maintained in line with the requirements of ISO27001.

Whereas the designated ‘owner’ of corporate information security risk within Invest NI rests with the Senior Information Risk Owner (SIRO), all risks are initially owned by the Division responsible for the area within which the risk falls. All risks will be reviewed by the project owner and they will be responsible for conducting and recording the risk assessment.

As information security risks are identified they will be analysed and evaluated using the methodology defined within this Policy. In addition, all information security related risk assessments should specifically identify:

- The risks associated with the loss of confidentiality, integrity and availability of information.
- The Controls that are necessary to implement the risk treatment which should then be compared to those contained within Annex A of the ISO27001 Standard to verify that no necessary controls have been omitted.

It is envisioned that the risk acceptance criteria (risk appetite) of risks to the ISMS will range from 'Cautious' to 'Averse' determined on a case by case basis subject to the risk assessment.

All risk assessment & treatment options chosen should be reflected in the Invest NI ISO27001 Statement of Applicability.

All major risks will be added to the Information Security Risk Register and will be reviewed by the Information Governance Group. Where a risk is deemed to have an organisational impact it will be escalated by the Information Governance Group to either the relevant Group Risk Register or, where applicable, the Corporate Risk Register.

For further detail on Information Security Risk Assessments and the process by which to escalate Divisional risk assessments on the Information Security Risk Register, please contact the Information Governance Manager via privacy.officer@investni.com.

6.0 FURTHER GUIDANCE

Risk management is not the responsibility of just a few specialists, it must be seen as a responsibility for all Board and staff members

While the Risk Management Team within the Performance, Compliance and Co-ordination Division can provide guidance on completion of risk registers and associated stewardship and assurance statements, ownership and responsibility for these rests with the respective project/divisional/group owner.

The Risk Manager, Colin Morelli, can be contacted at:

Address: Risk Manager
Performance, Compliance and Co-ordination Division
Invest NI
Bedford Square
Bedford Street
Belfast BT2 7ES

Telephone: 028 9069 8164
Email: colin.morelli@investni.com

Additional information on risk management processes can be found at the links below:

The Orange Book: Management of risk – principles and concepts *(2004, HM Treasury)*	https://www.gov.uk/government/publications/orange-book
Northern Ireland Audit Office: Good Practice in Risk Management *(2011, NIAO)*	http://www.niauditoffice.gov.uk/a-to-z.htm/report_good_prac_risk_management

Annex A – Risk Appetite/Escalation Scenarios

Scenario	Description	Appetite	Likelihood	Impact	Risk Rating (Residual)	Action
1	**IF** petty cash is lost **THEN** it must be recorded as a loss **RESULTING IN** accounts write off	Minimalist	2	1	2	No escalation required Manage risk within Division
2	**IF** ministerial support is lost **THEN** funding could be cut **RESULTING IN** failure to achieve PfG targets	Minimalist	3	2	6	Escalate to Corporate Risk Register Reassess risk at Corporate Level
3	**IF** EDO's are not managed **THEN** public funds could be used incorrectly **RESULTING IN** increased financial scrutiny and possible PAC interest	Cautious	3	2	6	No escalation required Manage risk within Division
4	**IF** Information Management is not adhered to **THEN** data could be used incorrectly **RESULTING IN** customer dissatisfaction	Cautious	3	4	12	Escalate to Corporate Risk Register Reassess risk at Corporate Level

Annex A – Risk Appetite/Escalation Scenarios

Scenario	Description	Appetite	Likelihood	Impact	Risk Rating (Residual)	Action
5	**IF** staff are not sufficiently engaged **THEN** workforce motivation will drop **RESULTING IN** drops in quality and poor customer satisfaction	Open	3	4	12	Exec. Director F&O decides if risk needs to be escalated to Corporate Risk Register. If not escalated can be managed within Division
6	**IF** external communications fail **THEN** INI objectives will not be fully understood **RESULTING IN** poor stakeholder engagement	Open	4	5	20	Escalate to Corporate Risk Register Reassess risk at Corporate Level
7	**IF** £4m investment fails **THEN** public funds will be lost **RESULTING IN** national press and PAC interest	Hungry	5	5	25	Recorded on Corporate Risk Register Managed at Divisional/Group Level

Annex B

Stewardship Statement

(Executive Leadership Team/Directors' Letter of Representation on the Risk Management Process)

To: **Senior Management Team**

From: **ELT Member (Name)/Director (Name)**
Executive Director (Group Name)/Director (Divisional Name)

As Executive Director of (name of Group)/Director of (name of Division), I am responsible for co-ordinating risk management activities within this Group/Division. This includes ensuring that the Senior Management Team is regularly updated on progress, chairing discussion of risk at Group/Divisional management meetings and developing communication to staff.

I am satisfied that, within (name of Group/Division) the following areas are on course for the achievement of objectives and that there are no known areas of concern, other than those specified, in my area of responsibility.

- There is an ongoing process for identifying, evaluating and managing the Group/Division significant risks.

- Risk registers have been developed for significant areas of the Group/Division and describe the significant risks and how the risks are managed. They are also used as a basis for regular reviews of the risk profile and reporting to the Senior Management Team.

- The status of risk is discussed at Group/Divisional management meetings including the review of risk information and risk indicators, any early warning signs of risks materialising and/or escalating, and any significant control failings or weaknesses.

- The risk management process has been in place since 31st December 2002 along with revised process since 31st December 2011.

Following my assessment of the risk management process and internal control framework within my area of responsibility, I am satisfied that controls are in place or being put in place to mitigate against the risks identified other than disclosed below:

Annex B

Signed:

Title: Executive Director, (name of Group)/ Director (name of Division)

Date: