



Risk Management Handbook



OWNER:	ILF Scotland SMT
AUTHOR:	R2
DATE DRAFTED:	Oct 2020
DATE APPROVED:	
VERSION:	1.1
STATUS:	Final

Revision History

Date	Version	Author	Comments
08/06/2022	1.1	JL	Updated appetite & tolerance statements

Review/Approval Register

Name	Position / Role	Review / Approval
Nadeem Hanif	Head of Finance	Review
Paul Hayllor	Senior Information Risk Owner	Approval

Table of Contents

INTRODUCTION	1
RISK MANAGEMENT PROCESS.....	1
RISK CONTROLS & TREATMENT.....	2
ANNEX A – RISK MANAGEMENT PROCESS	8
ANNEX B – RISK REGISTER GUIDANCE.....	9

INTRODUCTION

This Handbook is a practical guide for the management of risk in ILF Scotland; it details the end to end risk management process. The Handbook will support risk owners and other responsible persons in the successful management of risk thereby helping to reduce the severity and likelihood of threats to ILFS strategic objectives.

This Handbook should be used in conjunction with:

- The ILFS Resilience Framework;
- The ILFS Risk Management Policy;
- The ILFS Risk Register.

RISK MANAGEMENT PROCESS

1.1 Process & Flow

The ILFS risk management is set out at Fig 1; its purpose is to identify the risk, understand the degree of threat or opportunity posed, implement appropriate risk treatments, monitor and reassess the risk and controls in place. All of this activity is regularly communicated as part of ILFS’s ongoing vigilance and assurance as a key component of the ILFS Resilience Framework. The practical flow of this process is summarised in the Risk Management Aide Memoire at **ANNEX A**

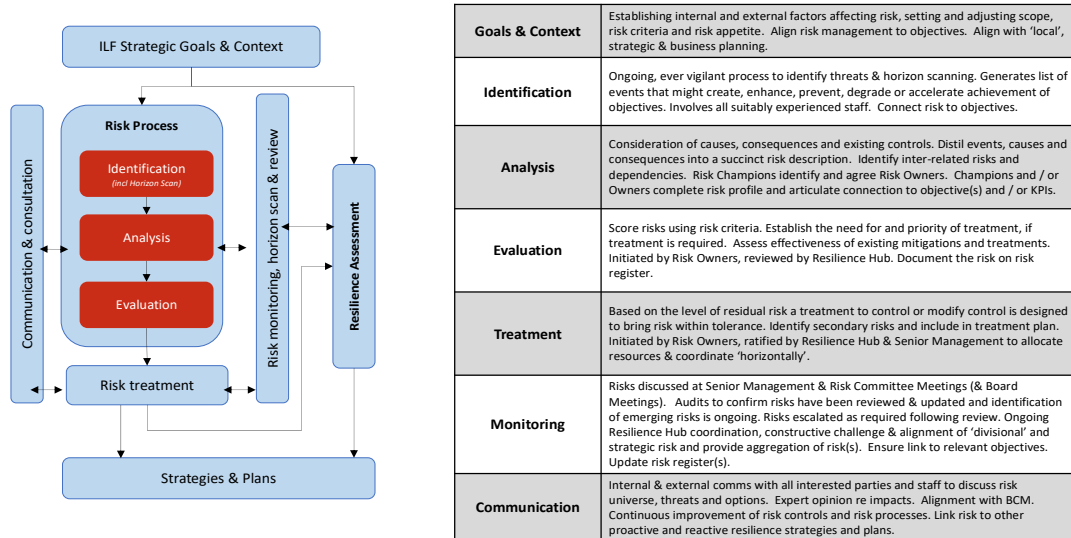


Fig 1: Risk Management Process

1.2 Risk Monitoring, Horizon Scanning & Review

Ongoing horizon scanning by ILFS Management and staff identifies emerging (new) threats and risks or changes to the ILFS internal and external risk landscape that could have a bearing on risks (in terms of levels of impact and likelihood) and therefore their management.

In parallel, existing (known) risks are kept under review on an equally ongoing basis; the effectiveness of controls in place to mitigate the risk are reviewed to ensure the controls contain the risk within appetite and tolerance, or within other

stated boundaries. Risks may also decrease, lose relevance or disappear, in which case their 'downgrade' or removal must also be monitored and discussed in the same way as 'new' or 'upwardly revised' risks.

1.3 Risk Identification

It is useful to have a systematic process in place to help identify risk and give assurance that you have a complete risk profile. A simple technique that provides a wide scan of areas that may affect objectives is PESTLES analysis (see table below):

Category	Examples
P olitical	Changes in policy; Committee decisions; Stakeholder relations.
E conomic	Financial constraints; Effect of global economy; Sustainability.
S ocial	Preventative effects; Demographic changes; Staff implications.
T echnological	Obsolescence; Cost of training & development; Efficiency.
L egal	EU requirements; Procurement processes; Accounting rules.
E nvironmental	Climate change implications; Changing environmental standards.
S ecurity	Physical assets; Information security; Data protection.

Table 1: PESTLES Analysis

Using PESTLES analysis categories to examine objectives will form a comprehensive risk profile for a given area of work. This can then be assessed and addressed. Reputation risk is included across the PESTLES categories. You will also notice that some of the examples above could be relevant in more than 1 area e.g. data protection. It is important that risks are not narrowly categorised, PESTLES is a tool to aid the risk identification that will flow from the breadth of knowledge and information available on the subject at hand.

Another simple method to help identify risk is to undertake a SWOT analysis on a particular piece of work, focusing on:



Fig 2: SWOT Analysis

- **Strengths:** internal attributes that are helpful to achieving an objective.
- **Weaknesses:** internal attributes that are harmful to achieving an objective.
- **Opportunities:** external conditions that are helpful to achieving an objective.
- **Threats:** external conditions that could be detrimental to performance. An

example:

Strengths	Staff experience; Management support
Weaknesses	Communication channels; Timescales
Opportunities	Stakeholder relations; IT developments
Threats	Geographic spread; Current culture

1.4 Risk Analysis

During this step the relevant manager, risk owner(s) and Resilience Hub work collaboratively (taking as long as they need / have, and moving quickly when required). They analyse the events, causes and consequences associated with this risk; in many cases there will be multiple causes, consequences and interdependencies. They articulate the connection to objective(s) and / or KPIs. All of these factors are considered in relation to the risk criteria. The aim of this step is to distil the long list of events, causes and consequences into a meaningful and manageable, well-classified and relevant list of risks. The logic of this distillation is demonstrated below.



Fig 3: Examples of Risk Analysis

Consideration is also given to existing controls and the succinct risk description is drafted. Risk Owners complete risk profile.

1.5 Risk Evaluation

A risk is evaluated on the combination of the consequences of an event (impact) and its probability (likelihood). The tables below provide a guide to risk levels and how they should be recorded in ILFS’s risk register format.

Impact: This is the estimated effect of the risk on the objective(s) in question. This is focused on scale, scope and resource implications.

Impact Score / Level	Finance –	Strategy	Compliance, Legal & Regulatory	Operations	Reputation & Credibility
1	Minor interruption. Leads to an impact of 1% – 2% of admin budget or award.	ILF Scotland not being able to meet its current service levels to the current numbers of applicants and disabled people	Even if incidents or compliance requests occur, the additional work activity remains within normal allocation to address or fulfil with no delays or extensions required which may lead to being reportable or damaging to audit requirements.	Some disruption to routine staff activities with limited duration (<1 day). No priority functions/activities impacted. No impact to payments. No overall time delay to the award cycle.	A letter of concern to the CEO from a single DPO, support organisation or individual initiates complaint handling protocols and direct intervention to resolve the issue (but is resolvable).
2	Leads to an impact of 5% – 10% of admin budget or award.	Level 1 plus ILF Scotland not being able to re-open the 2015 Fund nor grow the Transition Fund	1 -3 incidents per quarter where reporting requirements have exceeded their fulfilment time by up to 2 weeks as more staff time required than available.	Some loss of capability to service delivery with disruption to communication channels and delays to the award cycle not lasting more than 5 days. Some loss of core systems, people and ICT that prevent full line of business operations and back office corporate functions for up to 2 days. Ability to make payments not impacted.	Localised or sector specific expression of dissatisfaction with the actions of ILF Scotland leading to significant policy or practice changes or potentially disciplinary action. Issue remains resolvable but has caused temporary short term damage to reputation and credibility of ILF Scotland.
3	Leads to an impact of > 10% of admin budget or award.	ILF Scotland subsumed into either a new National Care Service or part of Social Security Scotland	> 2 requests/incidents per quarter have exceeded their fulfilment deadline by 2 weeks or more as more staff time required than available	Major service delivery failure with disabled people not able to contact ILF Scotland for more than 3 days. Significant negative impact on operations with >70% of staff unable to deliver normal activity. Most priority functions unavailable or affected. Ability to make payments adversely impacted.	Substantial adverse PR at UK national level on a one-off or sustained basis (spreading beyond local & social media). Likely to lead to a medium to long term loss of public trust and confidence in ILF Scotland.

Table 2: Impact Score Guide

Note: When assessing impact, consider, for example, the length of time services could be affected, how widespread the embarrassment could be for all business areas and how manageable the consequences would be.

Likelihood: This is the estimated chance of the risk occurring. This is focused on probability.

Likelihood/Probability Score			
4	3	2	1
Very Likely	Likely	Possible	Unlikely
Will undoubtedly happen on a frequent basis (expect almost daily).	Will probably happen/recur, but it is not a persisting issue/circumstances. Weekly or monthly.	Might happen or recur occasionally (several times a year).	Do not expect it to happen/recur but it may do so (annually at worst).

Table 3: Likelihood/Probability Score Guide

Note: The likelihood assessment should be determined by consultation and debate with stakeholders. The assessment should be based upon all available local knowledge of:

- Whether the event has occurred before, and how often
- Any changes in the area which may make the event more likely to occur
- Any analysis of trends or data available
- Any interdependencies

The table below provides a guide to the overall risk level based on multiplying the assessment of the impact and likelihood of a risk. This informs the risk scores recorded in ILFS’s risk register format.

Risk Profile	Score
Fully Managed	1 - 2
Improving	3-4
Stable	5 - 7
Materialising	8 -10
Crystallised	11-12

Table 4: Risk Profile Score Guide

If the risk poses a particular, unusual or fast moving threat to ILFS and /or objectives, it is escalated without delay (see 2.2 below).

Guidance for populating the Risk Register is at **ANNEX B**

RISK CONTROLS & TREATMENT

2.1 Control and Treatment

Once risks have been identified and assessed; the next stage is to decide what action needs to be taken to address the highlighted risks. Risks can be dealt with in four main ways, depending on the kind of challenge they present according to how likely they are to occur, and the impact if they did occur. In choosing between these responses, factors to consider include cost, feasibility, probability and the potential impact. Responses to risk can be to:

- **Tolerate:** for unavoidable risks, or those so mild or remote as to make avoidance action disproportionate or unattractive.
- **Treat:** for risks that can be reduced or eliminated by prevention or other control action e.g. new systems, altered processes, contingency plans.
- **Transfer:** where another party can take on some or all of the risk more economically or more effectively, e.g. sharing risk with a contractor.
- **Terminate:** for risks no longer deemed tolerable and where exit is possible e.g. elements of first class travel arrangements.

Where it has been identified that the risk landscape has resulted in a reduction of the levels of impact or likelihood, consideration should be made to reduce the level of mitigation and control, in order to release or refocus activity which could be beneficially redeployed elsewhere.

Conversely if the risk has been found to be escalating it would be expected that, where possible, further controls (treatment) will be applied to ensure the risk remains within appetite or tolerance. Where this is not possible the risk should be escalated for further consideration.

It is important to recognise that excessive caution can be as damaging as unnecessary risk taking. There may be opportunities to exploit a positive impact that might arise whenever tolerating, treating, transferring or terminating a risk i.e. where the potential gain seems likely to outweigh the potential downside.

Opportunities can be the correlation of threats when considering the uncertainty around objectives to identify risks:

Opportunity	Threat
We work more flexibly and make better use of technology to aid staff development and operational efficiency.	Staff numbers are reducing, and new IT systems require investment and training.
We demonstrate competence in government to strengthen reputation with stakeholders e.g. stamp duty and landfill tax.	New powers are being devolved to the Scottish Government, requiring new knowledge and skills, robust planning and implementation.

Current financial constraints are used as an energising factor to explore new areas of work and approaches.	Budgets have been reduced to a level requiring creativity to maintain service levels. This needs a framework and incentives to make it work.
More upfront investment to engage the wider Scottish public sector in extending shared service coverage: reducing costs and aiding efficiency targets.	Shared service coverage does not maximise resources and is difficult to maintain. Several public sector organisations are not engaged effectively.
We establish a flatter hierarchy to empower staff and increase engagement levels.	Staffing levels have fallen causing an imbalance in organisational structure.

The examples above illustrate how risk incorporates the opportunities in the uncertainty regarding the future and be a different way of looking at threats. Opportunities still require controls and actions to manage them, with the risk being that they will not be realised, or the cost of implementation outweighs the potential benefit.

2.2 Escalating Risks

Both strategic and local risk owners have the requirement to escalate risks that are either already, or are likely to exceed either thresholds or appetite or are close in proximity or fast moving. Risks that require escalation from the local / level will be escalated through the Management Team, Resilience Hub and onto Senior Management – the Aide Memoire at **ANNEX A** sets out the process.

When considering treatment options, the Resilience Hub and Senior Management can access resources to organise and direct the pan-ILFS treatment of risk where appropriate.

In practice when escalating risks, the initiator of the escalation should provide the rationale for the escalation along with opinions, options and timelines for consideration. The Resilience Hub can provide advice and support to both the initiator and those tasked to consider the escalated risk.

A diagram summarising the process is at **ANNEX A**

2.3 Performance

As well as monitoring the performance of individual risks and controls, Senior Management and the Audit & Risk Committee will monitor the performance of risk management to ensure it remains fit for purpose and is achieving the desired objectives, in accordance with the ILFS Resilience Framework. The Risk Management Committee shall formally review the performance of the system on an annual basis against the stated objectives and shall ratify or amend the system accordingly.

2.4 Risk Appetite and Tolerance

Risk Appetite Statements

Operations: ILF Scotland seeks new and emerging practices which may positively impact on internal efficiencies and improved operations. However, we have a **cautious** appetite for operational risk in relation to our priority functions, service delivery, support to disabled people and to our ability to make payments to disabled

people. Support, service and payments to disabled people are the overriding organisation priorities alongside staff well-being. All operations risk profiles should thus be ‘fully managed’, ‘improving’ or ‘stable’.

Compliance: ILF Scotland is **averse** to compliance risk. We require timelines and requirements for submissions and compliance related activity to be adhered to, and would expect priorities to be established to achieve this whenever required. All compliance risk profiles should thus be ‘fully managed’ or ‘improving’.

Finance: ILF Scotland is **averse** to financial risk, although we can accept a degree of financial risk in pursuit of our objectives. Individual risk taking should limit the impact to within 1-2% of the associated admin budget or award. All finance risk profiles should thus be ‘fully managed’ or ‘improving’.

Reputation and Credibility: ILF Scotland is **averse** to activities which may negatively impact on our credibility and reputation. In pursuit of being leaders in enabling independent living and being advocates for developing and sharing best practice across the public administration, we accept that sometimes we may be at odds with current accepted practice which may generate short term criticism or negative comment. We will always base changes and activity on a strong evidence base, that it is the right thing to do and will seek to address any specific complaints or negative reactions to our actions. All reputation risk profiles should thus be ‘fully managed’ or ‘improving’.

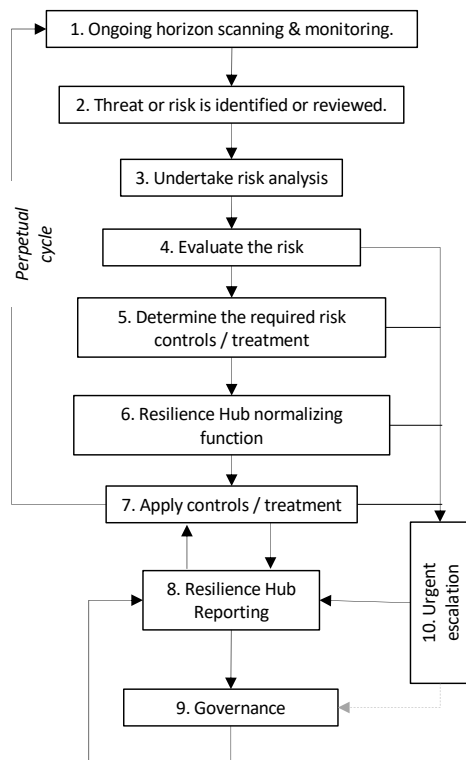
Strategy: ILF Scotland has a strategy that is bold and ambitious, therefore in some circumstances we would be more **open** to developing risks in pursuit of adding significant value to our current service or initiatives that would have a positive impact on our staff. However, a **cautious** approach would be taken where risks have the potential to impact negatively on the delivery of our service to disabled people. All strategic risk profiles should thus be ‘fully managed’, ‘improving’ or ‘stable’.

Risk Tolerances

Category	Finance	Strategy	Operations	Compliance and Reporting	Reputation and Credibility
Tolerance – we will tolerate a:	Level 1 impact	Level 2 impact	Level 2 impact	Level 1 impact	Level 1 impact

ANNEX A – RISK MANAGEMENT PROCESS

Risk Management Process Aide Memoire



Ref	Description	Responsible	Para
1	All staff always remain proactive in identifying risks as part of ongoing horizon scanning in relation to threats to objectives. These may relate to their direct area of responsibility or to any other area within ILFS. For known risks, the Risk Owner, Management Team, Resilience Hub and Senior Management (as appropriate) monitor the risk for any changes and / or any other consequences, including but not exclusively in the effectiveness of the controls. Known risks (and their controls) are monitored on a perpetual and frequent basis, according to the threat, proximity and clock speed associated with each risk; some may require constant vigilance.	All staff	1.1
2	The person identifying the change, threat or risk discusses this with the relevant member(s) of the Management Team and the Resilience Hub. Discussions start to determine causes and impacts but do not carry out detailed analysis or evaluation at this stage.	All staff Management Team Resilience Hub	Risk Policy, 1.2 & 1.3
3	The threat or risk is analysed with the appropriate member of the Management Team (either an appropriate manager(s) or the existing designated Risk Owner of the relevant risk(s)). They articulate the connection to objectives, identify inter-related risks and dependencies and consider causes, consequences and existing controls. The Owner completes the risk profile.	Management Team Risk Owner	1.4
4	Having clearly articulated the risk, the Risk Owner consults with relevant managers, staff and the Resilience Hub (as required) to evaluate the risk, using only the criteria stated in the ILFS Risk Policy. They score this risk as objectively as possible. At this point, the risk score may mean that the risk must be escalated to Senior Management immediately or at the next monthly update. As part of, or on completion of evaluation, the Risk Owner completes their update to the risk register and discusses this with the Resilience Hub and are prepared to defend their scoring if challenged.	Risk Owner Resilience Hub	1.5
5	The Risk Owner and Resilience Hub (and other relevant managers) consider how well existing resilience measures (proactive or reactive) control this risk. If the risk requires a control, or further treatment to improve an existing control then this need is clearly identified. At this point the treatment may be agreed (if simple), may require scoping and / or may require the approvals of Senior Management in order to prioritize and resource this consistently with other resilience activity. The Risk Register is updated accordingly.	Risk Owner Resilience Hub	2.1
6	At least monthly, and on an as required basis, the Resilience Hub reviews risks across ILFS to provide constructive challenge & coordination. Risks relevant to overarching strategic risks are aligned by Resilience Hub and / or are escalated if they exceed tolerances. Resilience Hub may challenge the risk assessment to provide a 'normalizing' function. Resilience Hub may also advise on the coordination of resource for effective treatment. Following Resilience Hub review, onwards escalation may be immediate or may be done in the normal run of the risk and performance cycle.	Resilience Hub	Risk Policy, Part 1 & 2
7	Controls are implemented as part of normal 'work' or projects. Treatments to improve existing controls may also be implemented. These actions are coordinated by Management, Risk Owners and the Resilience Hub. The effect of these controls on risk is monitored on an ongoing basis by the Risk Owner.	Risk Owner Management Team	2.1
8	On a routine basis (monthly / quarterly) the Resilience Hub report to Senior Management and / or the Audit & Risk Committee on both (a) the status of risks (individual and aggregated, as appropriate) and (b) the performance and effectiveness of the risk process (based on feedback from users). This reporting may be combined with reporting on the effectiveness of the resilience framework and the proactive and reactive resilience measures as whole. This reporting 'snapshots' the Risk Register on a routine basis; the register is consistently and routinely updated (not just for the reporting cycle), so ad hoc reports are also possible at any time, as necessary). Improvements to the system and to the controls will also be reported.	Resilience Hub	Risk Policy, 2.2 & 2.3
9	Senior Management, Audit and Risk Committee and the Governance Board, set direction in relation to objectives, priorities, risk appetites and operational impact tolerances. They seek assurance and challenge the functioning of the risk process and examine relevant risks in detail. They decide what resilience enhancements to make and what risks to accept.	Senior Management Resilience Hub	Risk Policy
10	If a risk poses a significant threat, has changed significantly or requires urgent consideration it should be escalated outside the 'normal' cycle of reporting and governance for immediate consideration. This may include triggering reactive resilience measures.	Management Team Resilience Hub	2.2

ANNEX B – RISK REGISTER GUIDANCE

3.1 The risk register format is based on an internationally recognised risk register model. The content has been kept simple, is in Excel format, uses drop down menus where appropriate (to aid completion) and allows information to be filtered as appropriate for flexible reading and reporting.

3.2 This is a standard format for risk registers across the Public Sector. Standardisation enables an accurate comparison and contrast of risks across the organisation, as well as improved information flows on risk in the organisation.

Process:

3.3 The process of adding and reviewing risks is detailed below:

- Once a risk has been analysed and evaluated it must be input onto the risk register by the Risk Owner.
- When inputting a risk, the Risk Owner must complete the columns in the risk register (below)

Risk Register Columns

Strategy Risks														
Ref	Description of Risk (Causes and Consequences)	Inherent Risk			Addressing the Risk via:	Mitigating Actions	Comments from Last Review	Residual Risk			Responsible Manager			
		Impact	Probability	Risk Profile Score				Inherent Risk Profile	Impact	Probability		Risk Profile Score	Residual Risk Profile	Risk Movement
15	ILF Scotland operates in a difficult strategic environment where: 1. Some key statutory partners would prefer local control over ILF resource. 2. Opinion 'hardens' against the	3	3	9	Treat	Systematic engagement and communication with key stakeholders is a routine part of ILF Scotland's operations. We regularly meet with:	Implementation of SLW for ILF recipients has had a negative knock on impact for some LAs, due to parameters of current policies. This is being managed via the review process. We are about to implement the next	3	2	6	6	6	6	CEO

Risk ref: is a helpful reference and can include links to objectives or outcomes.

Risk Description: should be a short summary of the risk, focusing on cause and impact i.e. what is the specific area at risk and how will it impact on objectives.

Inherent Risk Profile: this is the inherent risk score, the risk present without treatment/mitigation. The overall risk score is obtained by multiplying the impact and likelihood ratings.

Mitigating Actions: these are the actions that either have been taken, are being taken or will be taken in order to manage the risk.

Residual Risk Profile: this is the residual risk score, taking into account all the mitigating actions and comments from the last review. The overall risk score is obtained by multiplying the impact and likelihood ratings.



Risk Owner (Responsible Manager): This column is used to identify the most appropriate lead on any given risk. The purpose is not to assign all elements of managing a risk to one person but to ensure there is one point for coordination and reporting purposes.

Describing Risk

3.4 Risk is the uncertainty that may impact either positively or negatively on the achievement of objectives, represented by opportunities or threats.

3.5 In describing a risk for monitoring and reporting, it is helpful to consider cause and effect when defining a risk. This can focus the discussion on what action is required to manage a risk effectively.



3.6 It is important to take a progressive approach to describing risks – to focus on opportunities and present a more positive analysis of risk information. To represent the cause and effect, risk descriptions can be seen as a combination of ‘if’ and ‘then’ statements. A positive approach to describing a risk can be contrasted with a comparable negative:

	Example: [If] ‘We maintain and recruit sufficiently skilled staff [Then] resulting in clear timescales for priority assignments’.
	Example: [If] ‘We fail to maintain and recruit sufficiently skilled staff [Then] resulting in a bottleneck for priority assignments’.



3.7 This approach is to help counter the natural tendency to avoid risk and think purely of threats when analysing uncertainty. We should have more ambitious dialogue with colleagues and stakeholders on how we manage risk proactively. The emphasis of the risk does not change and leads to a consistent focus on the key phase of risk management: the actions being taken to achieve objectives.

3.8 In describing risks:

Avoid confusion between the impacts that may arise and the risks themselves e.g.

	Example: [If] “We improve project monitoring arrangements [Then] to meet revised performance targets.’
	Example: ‘Missing performance targets’.

Avoid defining risks as simply the converse of the objectives e.g.

	Example: [If] ‘Enhance key stakeholder engagement and communications [Then] to support changes to delivery programme’.
	Example: ‘Ineffective stakeholder relations’.

3.9 There can be a number of barriers to being innovative. For example, acting on new ideas and doing something different can be associated with increased risk. Whilst government has an important role in being accountable for the use of scarce public resources, this does not mean eliminating risk but rather tolerating and *managing* risk in order to achieve improved outcomes.

An Approach For Wording Risks

Capturing risk is something which we all do as part of the projects we work on.

Risk registers can vary greatly in terms of the language used and the level of detail they go into. Sometimes a risk is expressed as just a couple of words, which although may speak volumes to its author, does not always give enough information to all

relevant stakeholders - for example, 'content migration' or 'server load'. This ambiguous language can become a problem when it comes to rating the risk and to devise mitigation strategies.

We should all consider using the same process and language when adding/amending risks on the risk register. When describing a risk, consider:

There is a risk that...
Because...
Which could result in...

The first part ('There is a risk that') describes what the thing is that could happen. 'Server load' doesn't work in that sentence, but 'web server capacity could be exceeded on launch day' does.

The second part ('Because') tells the reader why it could happen. This is the essential part for rating the probability of the risk, and also when thinking of ways to avoid or manage the risk. To run with the server load example 'There is a risk that web server capacity could be exceeded on launch day because news of our product might go viral'.

The third part ('Which could result in') outlines what the consequence could be if that risk materialises to become an issue. This is important for rating the potential impact of the risk, and also for devising the strategies to deal with it. Therefore, if we carry on the same example:

There is a risk that web server capacity could be exceeded on launch day
Because news of our product might go viral
Which could result in people not being able to access the website or buy the product online due to browser timeout.