POCS31 Risk Management Policy
Scottish Legal Complaints Commission

Author:	**Neil Stevenson**
Recipient:	**Board**
Date:	**21 March 2017**

Table of Contents

1 Introduction

1.1 This document sets out the SLCC's policy on the management of risk.

1.2 A risk is a circumstance, event or factor that may have a negative impact on the operation of the SLCC or on its ability to achieve its corporate objectives. Risks can be the result of internal conditions, or external factors that may be evident in the wider business environment.

1.3 Risk management is the process or approach that seeks to eliminate or at least minimise the level of risk associated with a business operation. Essentially, the process should identify the situations that could result in damage to or ineffectiveness of any of the SLCC's resources (including staff and Members), identify the steps to remove, reduce or mitigate the effects of those situations and then take those steps.

2 Policy Principles and Approach

Principles

2.1 The SLCC will embed risk management in its corporate decision-making ensuring that the impact of policy decisions on risk is considered each time a strategic decision is taken or a policy is approved.

2.2 The SLCC will ensure that all processes and procedures are designed to minimise risk and the impact of risk.

2.3 The SLCC will foster a culture that embeds risk management into all aspects of its business, making it an integral part of the performance management system.

2.4 The SLCC will ensure that risk management is embedded in strategic, financial and business planning.

2.5 The SLCC will maintain strategic and operational risk registers that are reviewed and updated regularly.

Areas of risk

2.6 Having considered models used by Scott Moncrieff and KPMG (regulatory risk model) the SLCC has developed five key areas of risk:

1. Finance and best value
2. Political and policy
3. Quality and operational delivery
4. Legal and regulatory compliance
5. People
6. Opportunity and innovation

2.7 This updated policy does not include 'reputational risk' as previous policies have, as all of the above have reputational risk (which need incorporated in considering the risk) and because reputational risks too broad or undefined to link to one of the above were challenging to specify and mitigated, and therefore were not aiding in the effective monitoring and management of risk.

Risk Scoring

2.8 Risk will be scored on likelihood and impact.

2.9 A table in Appendix 1 sets out the scoring matrix

Appetite for risk

2.10 The SLCC is a statutory body and carries out a formal adjudicative function. As such, our risk appetite will usually be low. By this we mean that we would seek to minimise or reduce risk as far as possible and direct resources to making our operating environment as low risk as practicable, balancing the costs of mitigating or removing risk with the impact and likelihood of it.

2.11 However, in certain areas the Audit Committee and Board may set a higher appetite where this is deemed necessary to meet a justifiable need in the effective and efficient delivery of our functions.

2.12 Having considered models used by Scott Moncrieff and KPMG (regulatory risk model) six potential levels of risk appetite have been identified as appropriate to the work of the SLCC. More details on these are provided in Appendix 2.

Risk Tolerance

2.13 In setting appropriate mitigations forms of tolerance will be considered. The tolerance level will take into account the nature and impact of the risk and cost of controlling it.

Tolerate

2.14 Monitor the risk but take no action because either; the likelihood and impact are acceptable or because there is no cost-effect control. Risks that are tolerated are usually supported by a contingency plan to mitigate the effects should the situation arise.

Transfer

2.15 The risk will be transferred to another party outside the organisation. For example, contracting out a business function.

Terminate

2.16 Close down the business function or activity.

Treat

2.17 Take action to manage the risk through control measures.

Ownership of risk

2.18 The overall strategic risk register is owned by the Board and Accountable Officer (CEO).

2.19 Operational risk is owned by the Management Team and each risk will have a named responsible manager. In relation to complaints decisions for which they are responsible, the Board. The Management Team will ensure that all staff participate in the management of risk whether through direct ownership or through application of policies and procedures.

Control of risk

2.20 Controls are the measures or procedures put in place by the SLCC to manage or mitigate the risk or impact of risk. There are four categories of risk control. Every risk identified should have a control measure and some may have more than one.

Directive

2.21 A specific action or series of actions to ensure that a particular outcome is achieved. This could include, for example, actions to terminate risk, put in place a detective control or reduce the likelihood of risk.

Preventative

2.22 Action designed to prevent or reduce the likelihood of the situation giving rise to the risk occurring in the first place.

Detective

2.23 Action designed to identify when a risk is realised and is impacting or likely to impact on the SLCC.

Corrective

2.24 Action to correct the impact of risk realised.

Line of defence

When setting mitigations consideration will be given to the level of defence a mitigation is likely to give if effective:

1st line	stops a problem before it occurs / highly preventative / clearly measurable outcome
2nd line	a check likely to pick up an issue internally / demonstrates a commitment to prevention (such as taking advice prior to action) / outcome of mitigation may not be fully measurably
3rd line	An external check or assessment / minimisation of issue post-event

3 Reporting and Assurance

Assurance

3.1 Risk is ultimately owned by the Board. The Board receives assurance that risk is being monitored and managed appropriately from:

- The Audit Committee (AC)
- The CEO
- The Management Team
- Internal and External Auditors (regular audits and ad hoc, specific audits)

3.2 The sources of assurance are:

- AC annual report
- Risk register
- Management reporting
- Key Performance Indicators
- Feedback from staff and other stakeholders

3.3 For each strategic risk the following will be reported:

- Definition and details of risk
- Gross (inherent) risk
- Current / ongoing mitigations
- Net (residual) risk – after current/ongoing mitigations
- Target risk (what is being aimed for)
- Planned or further mitigations to assist in meeting the target risk

Review

3.4 Risk is proactively managed through monitoring and review of activity associated with or impacting on risk and its management. Review is managed through:

AC

3.5 AC will monitor and review risk through the monitoring of the strategic risk register and outputs of internal and external auditors. The AC will also have access to operational risks registers should they require them

3.6 Where necessary, AC will direct the CEO and Management Team to take appropriate action or refer issues to the Board for discussion and policy decisions, particularly in relation to operational risks directly in relation to the Board.

3.7 AC will report annually to the Board to give assurance that risk is being appropriately managed.

CEO

3.8 The CEO will report to AC through review of the strategic register and in bringing ad hoc risk issues to the attention of AC outwith the regular reporting cycle.

3.9 The CEO is responsible for ensuring the strategic risk register is reviewed and updated regularly as part of the assurance to AC and the Board.

3.10 The CEO is also responsible for monitoring and managing the operational risk register(s).

Management Team

3.11 The Management Team will report to the CEO and AC and provide assurance through reporting on action taken and its effectiveness.

Internal and External Audit

3.12 Auditors will bring to the attention of the Management Team, CEO and AC areas of risk and report on the effectiveness of the SLCC's risk management. Auditors will also provide advice and guidance in relation to risk management and specific areas of risk.

Review

3.13 AC will report to the Board quarterly in line with the agreed business cycle.

3.14 The CEO will report annually to AC on risk management activity and process in line with the agreed business cycle.

3.15 The CEO and Management Team will report quarterly to AC through the strategic risk register (and where appropriate the operational risk register).

3.16 The Management Team will review the risk register quarterly.

3.17 Risk owners will review and update the risk register on an ongoing basis.

3.18 Internal and External Audit will report on risk through the agreed audit programmes.

Risk Register

3.19 The 'risk register' is a generic name for a series of documents that collectively enable a proactive approach to identification and management of risk. It consists of:

Strategic Risk Map

3.20 This is a reporting tool that enables the SLCC to take an overview of strategic risk. It is a visual representation of the overall risk position and informs the SLCC whether its risk map is consistent with its appetite for risk. It is derived from the strategic risk register. The strategic risk map is owned by the Board and CEO and monitored and reviewed by AC.

Strategic Risk Register – detailed information sheets

3.21 A detailed set of information sheets, one for each individual risk, setting out all the information required under this policy.

Strategic Risk Register – risk summary

3.22 A numbered summary of the identified strategic risks, their likelihood of occurrence, their impact and which operational risks contribute to these factors. The aim is to keep this at a strategic level, linked to the corporate strategic objectives. It is the overarching document into which other registers feed. The strategic risk register is owned by the Board and CEO and monitored and reviewed by AC.

Operational Risk Register

3.23 A numbered summary of operational risks that collectively feed into the strategic risk register. The operational risk registers will also be supported by appropriate Board, Management Team and Audit Action logs.

3.24 The risk register is a living document. It must be reviewed quarterly and should be updated by risk owners on an ongoing basis.

3.25 Direct reference should be made to numbered risks when reporting to the Board, seeking decisions from the Board or seeking approval for policies.

4 Summary of Roles and Responsibilities

4.1 Roles and responsibilities are summarised as:

Party	Responsibility	Role	Frequency of reporting
Board	• Ownership of SLCC risk and risk policy	• Approve risk management policy • Assurance that policy is applied and strategic risk is managed effectively	As required to external and internal stakeholders
Audit Committee	• Monitoring of risk management activity • Providing assurance to the Board	• Oversee and monitor the risk policy and risk management activity. • Review the strategic risk register (and on request, the operational risk register) • Direct the CEO and Management Team as appropriate • Provide support and advice to the CEO and Management team as appropriate	• Annually to the Board
CEO as Accountable Officer	• Shared ownership of risk • Management of risk • Providing assurance to AC	• Ensure that risk registers are updated and reviewed regularly • Own and manage the operational risk register • Report and provide assurance to AC • Ensure risk is managed in line with the risk registers and other direction from AC and/or the Board • Ensure that staff and managers are appropriately briefed and trained to manage risk	• Quarterly to AC • Annually to AC
Management Team	• Shared ownership of risk • Management of risk • Providing assurance to AC and CEO • Operational ownership of specific risks	• Ongoing updating of the operational risk register for owned risks • Quarterly reporting and review of the risk register to CEO, Management Team and AC • Ensure staff are aware of risk, that it is embedded in processes and performance management and that staff are appropriately trained to deal with risk.	• Quarterly to AC • As required to CEO
Internal and External Audit	• Report and advise on risk to AC and CEO • Provide assurance to AC	• Carry out and report on audits to the programme agreed with the SLCC • Give appropriate advice to the SLCC at all levels in relation to risk management • Bring concerns about risk to the attention of the CEO and AC	• As agreed through audit programme
All staff	• Operational management of risk through application of policies and procedures	• Contribute to the management of risk through applying policies and procedures appropriately and consistently • Raise concerns or identified risk with line management, CEO, Management Team or Board as appropriate.	• As required by line management

Appendix 1 – Scoring Template

LIKELIHOOD / IMPACT	1 - VERY UNLIKELY • *Unlikely to occur except in rare or exceptional circumstances* • *May not have happened before.*	2 – SLIGHT • Slight risk but could occur. • *Limited evidence of such risk occurring elsewhere.*	3 – FEASIBLE • *Possibility of occurring in near future.* • *Limited evidence of immediate threat.*	4 – LIKELY • *More likely to occur than not.* • *May become frequent.* • *May have occurred at some regulators/complaints bodies*	5 - ALMOST CERTAIN • Imminent or high probability • *Has happened before and recently* • *May have occurred to many regulators/complaints bodies*
5 –CRITICAL •*Critical threat to a strategic aim or operational priority* • *Exposure to risk to client safety* •*Threat to viability of major activity, process, or relationships* •*Critical impact on long term organisational effectiveness and/or reputation.*	**5**	**10**	**15**	**20**	**25**
4 –MAJOR • *Major threat to strategic aim or operational priority* • *Major activities or processes may struggle to deliver key milestones.* •*Major impact on medium term organisational effectiveness.*	**4**	**8**	**12**	**16**	**20**
3 –SIGNIFICANT • *Significant threat to strategic aim or operational priority* • *Causes problems for activity or process, but manageable.* • *Short term impact on organisational effectiveness* • *Reputational damage if it persists.*	**3**	**6**	**9**	**12**	**15**
2 –MINOR • Minor threat to strategic aim or operational Priority • Limited delay or impact on activity or process • Short term impact on organisational effectiveness.	**2**	**4**	**6**	**8**	**10**
1 –NEGLIGIBLE • *Negligible threat as long as regular monitoring shows no change.* • *Limited delay or impact on activity or process* • *No significant impact*	**1**	**2**	**3**	**4**	**5**

Appendix 2 – Risk Appetite Definitions

	Avoid	Minimal (ALARP	Caution	Open	Seek	Mature
	Avoidance of risk and uncertainty is a key organisational objective	*(as little as reasonably possible) Preference for ultra-safe business delivery options that have a low degree of inherent risk and only have a potential for limited reward.*	*Preference for safe delivery options that have a low degree of residual risk and may only have limited potential for reward.*	*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 (and value for money etc.)*	*Eager to be innovative and to choose options offering potentially higher business rewards, despite greater inherent risk.*	*Confident in setting high levels of risk appetite because controls, forward scanning and responsive systems are robust*
1. Finance and best value	Avoidance of financial loss is a key objective. We are only willing to accept the low cost option as best value is our primary concern	Only prepared to accept the possibility of very limited financial loss if essential. Best value is the primary concern.	Prepared to accept possibility of some limited financial loss. Best value still primary concern, but willing to consider other benefits or constraints. Resource generally restricted to existing commitments	Prepared to invest for return and minimise the possibility of financial loss by managing the risks to a tolerable lever. Value and benefits considered (not just cheapest price). Resources allocated in order to capitalise opportunities	Investing in the best possible return and accept the possibility of financial loss (with controls in place). Resources allocated without firm guarantee to return – 'investment capital' type approach	Consistently focussed on the best possible return of stakeholders. Resources allocated in 'social capital' with confidence that the process is a return in itself
2. Political and policy	Play safe, avoid any confrontation of challenge of status quo	Play safe, avoid any confrontation of challenge of status quo unless on minor technical or legal changes	Play safe, broader changes considered but only changes likely to have support / or no opposition from all stakeholders	Risk / benefit analysis; changes considered positive for SLCC will be considered even if some likely opposition	Risk / benefit analysis; changes will always be pursued where positive for SLCC, even if some / significant likely opposition	Seeking leadership role in political and policy thinking through radical commentary on potential for change..
3. Quality and operational delivery	Avoidance of anything that could compromise quality	Only prepared to accept the possibility of very limited negative impact on performance against quality standards. Fairness is the primary concern	Prepared to accept possibility of some limited deterioration in performance against quality standards. Willing to consider other benefits linked to adverse performance where fairness is not compromised.	Prepared to consider metrics and performance and the benefits and constraints of meeting targets whilst managing associated risks to a tolerable level. Fairness to be considered first to ensure any decisions do not compromise.	Prepared to take a degree of risk when pursuing a new of innovative course of action to help improve performance and willing to accept the possibility of performance deterioration (with controls and checks in place for fairness)	Consistently focussed on pursuing new or innovative courses of action to deliver best in class performance. Willing to take risks to do so. Willing to accept performance deterioration as new approaches are tested (within controls and check in place for fairness)
4. Legal and regulatory compliance	Play safe, avoid anything which could be challenge, even unsuccessfully	Want to be very sire we would win any challenge. Similar situations elsewhere have not breached compliances.	Limited tolerance for sticking our neck out. Want to be reasonably sure we could win.	Challenging would be problematic, but we are likely to win it and the gain will outweigh the adverse consequences.	Chances of losing any are real and consequences would be significant. A win would be a great coup.	Consistently pushing back on regulatory burden. Front foot approach informs better and more proportionate regulation
5. People	Defensive approach to people management – aim to maintain within headcount allocations and maintain current roles rather than create of	Workforce innovations avoided unless essential or proven track record elsewhere	Tendency to stick to status quo in terms of workforce planning, innovations and new approaches avoided unless really necessary and linked to leadership	Innovation supported, with demonstration of improvements in workforce output	Innovation and alternative approach pursued in order to challenge and change current practices and achieve improvements in workforce output and	Innovation and alternative approached pursued as a priority in order to challenge and change current practice and achieve improvements in

	innovate		management		engagement.	workforce output and engagement.
6. Opportunity and innovation	Defensive approach to objectives – aim to maintain or protect, rather than create or innovate. Priority for tight management controls and oversight with limited devolved decision authority	Innovations always avoided unless essential or commonplace elsewhere. Decision making authority held by senior management.	Tendency to stick to the status quo, innovations in practice avoided unless really necessary. Decision making authority generally held by senior management.	Innovation supported,. With demonstration of commensurate improvements in management control. Responsibility for non-critical decision may be devolved.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust rather than tight control.	Innovation the priority – consistently 'breaking the mould' and challenging current working practices. Devolved authority – management by trust rather than tight control is standard practice.
Appetite : **Acceptable level of residual risk**	**NONE**	**LOW**	**LOW**	**MEDIUM**	**MEDIUM**	**HIGH**