The Scottish Parliament
Pàrlamaid na h-Alba

Improving Risk Management
28 November 2022
Reference: LG (2022) Paper 060

Executive summary

1. This paper will set out how our approach to risk management will be refreshed. The end goals are to help risk management work be more relevant, current, visible, and consistent. The 4 main areas that will be considered are:
   a. Policy & Process:
   b. Capability Development
   c. Management Information, and
   d. Risk Culture:

2. This paper will not consider the management of specific risks.

3. Leadership Group are asked to:

   a. Note the structure and contents of this outline proposal, and
   b. Advise on areas to focus on, if any, in general risk management skills.
   c. Advise on priorities, impact, and other factors to consider when implementing the programme

Issues and options

4. At its meeting on 23rd May, Leadership Group endorsed an objective review of our approach to risk management and agreed on the support the resilience team would provide on this, namely:

   a. Supporting LG in ensuring that the risks “that matter” are represented in the strategic risk register.

   b. Shifting attention from retrospectively reviewing risk register content to identifying actions, controls and other initiatives that would demonstrate effective risk management.

c. Use the gap between tolerance and residual risk to prioritise effort

d. Refresh / re-publish our risk management policy

Maturity Model Assessment

5. As part of assessing where improvements could be sought, a Risk Management Maturity Model was shared with LG members and a few other relevant staff. Overall, the maturity model had 4 levels:
    a. Initial / Fragmented
    b. Novel / Organised
    c. Normalised / Influential
    d. Natural / Leading Groups

6. When looking at the entirety of our approach to risk, not just the strategic risk register, feedback suggested that we are predominantly at the "Novel / Organised" level, and we should at least aspire to the "Normalised / Influential" level. In time, we may wish to consider how we can achieve some aspects of the "Natural / Leading Groups" level, particularly in how we assess and consider the entirety of our risk landscape.

7. The maturity model and other work from the resilience team has indicated we can look at 4 main aspects of improving what we do on risk management.

Policy and Process

8. Risks can be and are routinely identified across the organization as part of office plans, project, and programme management and in the strategic risk register. There is advice in place across all those areas on what relevant officials should be doing as part of risk management but there may be improvements needed in engaging people on "why" we ask for risk management to be undertaken and what is required of that.

9. Consistency of identification and description needs supported and our policy and supporting tools will help achieve that. The "causes, impact, consequences" model already used in the strategic risk register will be rolled out across other risk management areas and it is very likely we will move away from using "likelihood" as a metric in assessing risk. Instead, we will look at how relative impacts and proximity/velocity (when subject matter experts anticipate the risk might occur) as the variables used to help prioritise effort.

10. The Resilience Team will specifically look at:
    a. Establishing / re-stating a risk management policy

b. Consider which types / levels of risk need to be considered by which layer of governance / management –

c. Re-stating the purpose of the strategic risk register and the criteria / justification for including risks that need to be managed at that level

d. By using a consistent method of describing and assessing risks we will allow more attention to be given to controls and mitigations and in setting target dates for when target / acceptable risk states will be achieved.

e. Ensuring risk management training, tools and other support focuses on helping relevant officials follow the policy

11. A draft policy can be found at Annex A

12. We will also reconsider our established High Impact Risks. It is very likely that the nature of these will have changed, and we will determine if the risks are still relevant, the appropriateness of controls and work with owners to ensure the risk profiles are updated as has already started with the Loss of Critical Supplier and Loss of Utilities risks. As a reminder our current set of High Impact Risks are currently:
    a. Loss of Access to Holyrood
    b. Loss of Access to Staff (& Contractors)
    c. Loss of Access to IT or Connectivity
    d. Loss of Access to Members
    e. Loss of Utilities
    f. Loss of a Critical Supplier
    g. Loss of Information

Capability Development

13. We will establish twice yearly risk horizon scanning sessions with Office Heads where the Resilience Team will present a view on emerging risks. Office Heads will be asked to consider and discuss with their Group Head. This will feed into Leadership Team discussions on horizon scanning and emerging risks.

14. As noted earlier, staff across the Parliament have risk management as part of their duties. There is “vocational” training available to those who seek qualifications or CPD in fields such as project management and procurement which will undoubtedly help in developing skills, but this may create a bit of an imbalance between those who do not have routine access to such support.

15. This imbalance will be off set in some measure through support from the Resilience Team at horizon scanning sessions, other themed briefings and via updated guidance and templates. **Leadership Group are asked to consider what, if any, further effort should be given to direct**

development of risk management capability in relevant staff via training (classroom, e-learning etc).

16. If dedicated training is recommended, we will aim to have that and other materials available to support the next iteration of Office and Budget planning activities over late summer and early autumn 2023.

Management Information

17. A great deal of work has gone into risk management templates across the Parliament. Any work we look at now needs to ensure we maintain the usability and purpose of these templates and be mindful that any improvements do not accidentally take away current usefulness. Changes will focus on consistency of risk descriptions, clarity on when target / acceptable risk assessments will be achieved and making it easier to aggregate and combine information for review purposes.

18. Like most organisations we mostly use spreadsheets for the recording of information. This is straightforward for most as many of us have some familiarity with how these operate and navigation around a typical risk register spreadsheet is generally not too difficult. What these tools don’t allow – or, at least, don’t readily enable - is aggregation of information or automation of workflows and presentation of management information or presentation of the whole risk network.

19. We have seen how other organisation use already paid for services from their Microsoft 365 estate and we will take advice from BIT on how we can adopt a similar approach when resources permit. The resilience team will “prototype” what this might look like where limited skills and limited time allow.

20. If / when we do transition away from spreadsheets, a key factor will be aiming to ensure that stakeholders can update information as easily as they can with current mechanisms.

Risk Culture

21. There is a predominance for risk management activity to be seen as a standalone, imposed, regulatory- or compliance-driven activity. That is the case with us and with many other organisations. It is desirable to, over time, move to a position where risk management is more routine and prominent in day-to-day activities, is valued by risk owners and the time and effort undertaken by a range of officials is recognised and welcomed. This must be led from the top of the organisation and LG will be asked to

consider how best they can do that and what support they may need in doing so.

22. As well as identifying risks from our own activities we need to be aware of external factors that may disrupt what we do and, as noted earlier, we will seek to run twice-yearly horizon scanning sessions with output targeted towards LG.

23. We will also use “Resilience Week” type events on occasion to do distinct briefings on contemporary issues or invite expert, external speakers to share their experience of actual events or assessment on the current risk landscape.

Governance

24. The Group Head for Resilience and Sustainability, Lynsey Hamill, is responsible for the risk management strategy, policy and reporting framework. The Head of Resilience, Tommy Lynch, and the resilience team will be responsible for the day-to-day development and operation of the risk management framework across the Parliament and analysis of the information presented as part of that framework.

25. Identified risk, mitigation and control owners are responsible for the management of specific risks to the standards expected in our control environment.

26. Currently it is not anticipated that an overall EQIA will be necessary, but this will be completed routinely as part of the development of any training and other supporting materials.

Resource implications

27. Development of the policy, framework and any training materials will predominantly be resourced via the Resilience team and its Resilience training contract.

28. Development of improved risk management tools and preparation of management information reports will be taken forward when resources are available from BIT.

29. Additional time will be needed from those that have risk management as part of their day-to-day responsibilities, particularly in attending any training and other capability development events. As noted earlier in the paper, all training will be as targeted and focussed as possible.

30. Any additional time required from those with risk management responsibilities should be minimal given the effort already undertaken in

that area. Any changes in requirements and reporting will, of course, need some additional effort as those are adopted.

Publication Scheme

31. This paper may be published.

Next steps

2023 Q1	2023 Q2	2023 Q3	2023 Q4
• Engagement & Initial Horizon Scanning with OHs • Discussions with GHs on group-specific risks and support needed. • Revisit purpose of Strategic Risk Register • Updated strategic risk register with target dates fo achieving acceptable impact. • Initial discussions with HIR owners.	• Availability of Training Material • Updating Risk Templates • Prepare management views on risks and risk landscape	• Updated risk assessment used in Office Planning & budget bid process • Further development of management information	• Review as part of Resilience Annual Report • Objective Setting for 2024

Decision

32. Leadership Group are asked to:

   a. Note the structure and contents of this outline proposal, and
   b. Advise on areas to focus on, if any, in general risk management skills.
   c. Advise on priorities, impact, and other factors to consider when implementing the programme

Resilience Team
28th November 2022

Annex A

Draft Risk Management Strategy & Policy

Introduction

Consistent and effective risk management can help provide reassurance to all our stakeholders that we take steps to keep people safe, to make better decisions and to maintain core activities when our operating environment changes or is disrupted.

Our approach to risk is designed to help identify, assess, manage, and monitor risks and, in so doing, support delivery of our Session 6 Strategy and the objectives within that strategy.

Strategy

Risk Management in the Scottish Parliament will:

- Continue to form a core component of excellent corporate governance and management practices.
- Provide a sound basis for integrating risk management into decision-making.
- ensure that appropriate mitigating actions are in place to manage identified risks.
- Help ensure that the objectives of the Scottish Parliament are not adversely affected by significant risks that have not been anticipated.
- ensure achievement of outputs and outcomes and having reliable contingency arrangements in place to deal with the unexpected which may put service delivery at risk.
- ensure periodic assessment of the Scottish Parliament's attitude to and appetite for risk; and
- promote a more innovative, less risk-averse culture in which the taking of appropriate risks in pursuit of opportunities to benefit the Scottish Parliament is encouraged.

The management of risk will continue to be an integral part of the Parliament's Strategy and of our Office Plans.

Our principles

As part of our planning and delivery process, our principles are to:

- Integrate with our values, particularly Excellence and Stewardship
- Align with outcomes – being responsive to change to achieve objectives

- Engage stakeholders – recognising capabilities to help or hinder outcomes
- Provide clear direction – understanding roles and responsibilities
- Inform decision-making – linking with business planning and monitoring
- Enable continuous improvement – using lessons identified to develop what we do
- Create a supportive culture – embracing considered risk-taking
- Achieve measurable value – using resources effectively, improving governance.

Our approach to risk management

Values

As well as supporting better decision making and planning, we will ensure that our approach to risk management aligns to our values, in particular:

Excellence

We will strive to make sure our approach is aligned with good practise and that we learn from trusted colleagues outside the Parliament on how to improve what we do.

Stewardship

Our approach to risk management will contribute to minimising impact and sustaining Parliament activities when faced with disruption to, or changes in, our operating environment.

We will help colleagues to adopt a positive approach to managing risk, including:

- Providing training and support to help identify risks in a consistent manner and to manage resultant risk mitigation actions and controls
- Operating a risk management process that is proportionate, easy to understand, easy to use and built on good practise
- Championing risk management across the Parliament and encouraging routine risk management discussion where that will add value.