Registers of Scotland

RoS Board

December 2021

Key risk register 2021-26 (KRR)
Risk management policy

Purpose

1. The purpose of this paper is to provide RoS Board with an update on the KRR 2021-26 following EMT and Audit & Risk Committee (ARC) reviews and continuous Key Risk Owner (KRO) reviews.

2. The paper supports the board in fulfilling its role to provide strategic advice to the Keeper for its focus on setting a framework of prudent and effective controls that enables risk to be assessed and managed.

Recommendation

3. RoS Board is requested to review:

   a. the KRR summary at Annex 1

   b. the Cyber Resilience update at Annex 2

and advise the Keeper on the update.

4. RoS Board is requested to review the Risk Management policy at Annex 3 and advise the Keeper and EMT.

Background

5. RoS KRR contains the key risk scenarios that may affect delivery of our corporate plan objectives and the risk response strategies for these threats and opportunities. The KRR is a 'live' document which is reviewed and updated at least monthly by KROs and submitted to EMT for approval as part of their monthly corporate governance review process. The KRR is also submitted to RoS Board and ARC meetings for noting and/or advice as a summary report or as the RoS Assurance Framework report.

6. The Risk Management policy is owned by EMT and is reviewed annually by EMT, PCS Trade Union, the ARC and the RoS Board.

Key risk register (KRR) reporting format

7. The paper continues the 'reporting by exception' approach approved at the September 2021 RoS Board meeting, comprising 3 elements:

Reporting element	Frequency of reporting	Board input / 'Ask' of the Board
1. RoS Key Risk profile	Every Board meeting	Advice on whether strategic risk exposure continues to be captured by KRR 2021-26
2. New/developing risks	As relevant	Advice on how risks have been assessed in terms of 'causes - risk scenario - impacts' and the risk response (i.e. controls)
3. Risks trending away from target risk score / controls not delivering anticipated risk response	As relevant	Advice on how risks have been assessed in terms of 'causes - risk scenario – impacts' and the risk response (i.e. controls)

Key risk register – reporting element 1

8. KROs have reviewed the KRR and updated risk descriptions, appetite, proximity, scoring, controls and assurance opinions. A summary of the KRR as at the date of this paper is at Annex 1. The 'Live' KRR will be available to RoS Board at its December 2021 meeting.

Key risk register – reporting element 2

9. The "People and Change" opportunity in KRR 2020-25 was re-framed as a threat in KRR 2021-26. A first draft of the re-framed risk was presented at the September Board meeting. Following ongoing EMT review and Board feedback the risk is being developed further, with a second draft being prepared.

10. This draft simplifies the set of risk causes by focussing on the 'organisational needs' element of the risk scenario. Controls are being reviewed to better distinguish between (i) strategic controls (likely to endure indefinitely and responding as organisational needs change over time) and (ii) their component parts.

11. The risk scenario, key risk owner, risk appetite, risk scoring and impacts remain as assessed in the first draft.

12. ERM will continue to support the KRO and control owners in defining a 'route to target' for this risk (involving development of the strategic controls), enabling reporting by exception at future Board meetings.

13. Annex 2 (Cyber Resilience key risk update) contains a summary of the high-level findings from the recent ADARMA (a third party professional services partner) report on cyber resilience at RoS. The report follows a series of technical and non-technical exercises designed to test our cyber incident response capabilities. The report identified areas of good practice and improvement opportunities, summarised in Annex 3 (with a summary of our proposed response). Enhancing our incident management capabilities (through these improvement opportunities) will reduce anticipated impacts associated with a cyber incident, and enable an overall reduction in the Cyber Resilience key risk score.

14. ARC will receive a more detailed presentation on the ADARMA report and response as a means of assurance at the February ARC meeting.

Key risk register – reporting element 3

15. Existing risk responses for all key risks continue to deliver the expected risk reduction effects. The ongoing introduction of new controls and/or enhancements to existing controls is continuing as planned in each risk's 'route to target'.

Risk Management Policy

16. The risk management policy is included for RoS Board review at Annex 3. The EMT approved timescale for 2021 annual review of the risk management policy is outlined below:

a. 24 September 2021 EMT CG meeting to complete review of a draft 2021 risk management policy and approve submission to the November 2021 ARC meeting for review and advice.

b. PCS comments requested for return by 15 October 2021.

c. 09 November 2021 ARC meeting requested to complete a review of the draft 2021 risk management policy, advise any recommended changes and/or approve submission to the 14 December 2021 RoS Board meeting for review.

d. 14 December 2021 RoS Board meeting requested to complete a review of the draft 2021 risk management policy, consider any ARC recommendations and/or advise further recommended changes and confirm any recommended changes to EMT.

e. December 2021 EMT CG to consider any PCS/ARC/RoS Board incorporated changes, complete final approval of policy and its publication on RoS intranet by end December 2021.

17. No changes to the policy have been proposed following review by EMT, PCS and ARC.

Conclusion.

18. RoS Board to review the KRR 2021-26 update and Risk Management policy at Annexes 1, 2 and 3 and consider the background, topic matter and recommendations in this paper for advice to the Keeper and EMT.

Head of Enterprise Risk Management
Corporate
29 November 2021

Annex 1 – KRR Summary

Threats

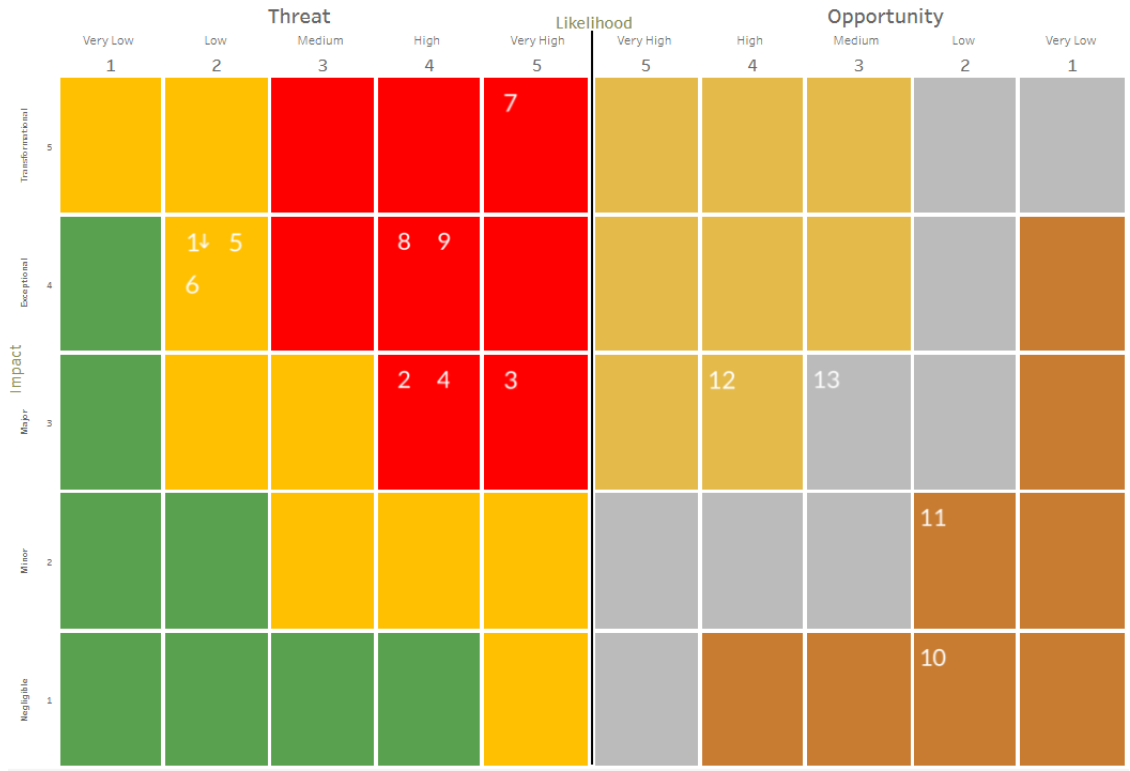
	Current Score	Target Score	Risk Appetite	Risk Response
1. Financial Health	8 ▼ 7 vs Inherent ▼ 4 vs Last Month	4	Minimalist	Treat
2. Financial Capability	12 ▼ 3 vs Inherent ↔ 0 vs Last Month	9	Cautious	Treat
3. Operational Capacity	15 ▼ 0 vs Inherent ↔ 0 vs Last Month	6	Cautious	Treat
4. LRC - Ministerial Target 2024	12 ▼ 0 vs Inherent ↔ 0 vs Last Month	4	Minimalist	Treat
5. Public Trust in the Registers	8 ▼ 2 vs Inherent ↔ 0 vs Last Month	4	Minimalist	Treat
6. Uncertainty of future business model beyond 2024	8 ▼ 0 vs Inherent ↔ 0 vs Last Month	6	Cautious	Tolerate
7. People and Change	25 ▼ 0 vs Inherent ↔ 0 vs Last Month	4	Minimalist	Treat
8. Cyber Resilience	16 ▼ 9 vs Inherent ↔ 0 vs Last Month	9	Cautious	Treat
9. Product Sustainability	16 ▼ 4 vs Inherent ↔ 0 vs Last Month	9	Cautious	Treat

Opportunities

	Current Score	Target Score	Risk Appetite	Risk Response
10. LRC - Realising Benefits	2 ▲ 1 vs Inherent ↔ 0 vs Last Month	16	Open	Treat
11. Maximising Use of RoS Data	4 ▲ 3 vs Inherent ↔ 0 vs Last Month	20	Open	Treat
12. Sustain and Improve Customer Experience	12 ▲ 11 vs Inherent ↔ 0 vs Last Month	20	Open	Treat
13. Relationship with SG	9 ▲ 8 vs Inherent ↔ 0 vs Last Month	16	Open	Treat

Risk Tolerance Thresholds for Threats and Opportunities

The combination of likelihood and impact rating provides a mechanism to prioritise risk response.



Annex 3

Risk Management Policy

Author	Head of Enterprise Risk Management		
Reviewed	Head of Risk & Information Governance		
Cleared	Corporate Services Director		
Approval	EMT	Approval Date	17/12/21
Policy Version	1.0		
Review Responsibility	RoS Board ARC PCS EMT	Review Date	14/12/21 09/11/21 15/10/21 24/09/21
Suitable for Publication	Y		
Contact:	rossecretariat@ros.gov.uk		

1 Purpose and Scope

1.1 The RoS Board and Executive Management Team (EMT) recognise that RoS will face a variety of risks in delivering its objectives.

1.2 This policy sets out RoS commitment to responding to the identified threats to achieving our objectives and opportunities for increasing likelihood of success.

1.3 In doing so, the Keeper, RoS Board and the EMT are also committed to supporting the benefits from deploying and resourcing an integrated enterprise risk management (ERM) framework for strategic, change and operational risks, set in the context of the Corporate Plan and risk appetite agreed by RoS Board and EMT.

1.4 This policy applies to all enterprise activities in RoS including all people, processes, premises, technology, information and supply chain activities.

2 Guiding Principles

2.1 The principles of this policy are to:

- ensure it is proportionate and fit for purpose in line with the Scottish Public Finance Manual (SPFM) risk management and internal control guidance
- ensure it is aligned to the context set by the Corporate Plan
- ensure it has a comprehensive scope covering all of our activities
- ensure it is embedded across the organisation
- ensure it is dynamic to respond to change

3 The Policy

3.1 RoS objectives for enterprise risk management (ERM) are to:

- provide appropriate risk information to support decision making at all levels
- assist in achieving economic, efficient and effective processes to achieve the best outcomes, reduced uncertainty and a supportive risk culture
- achieve compliance with our mandatory obligations

- provide assurance that our internal control activities and risk management practice comply with our risk management principles

4 Roles and responsibilities

4.1 The EMT is responsible for the content of this policy, its approval and review, which includes the RoS Board and its Audit & Risk Committee (ARC). They are responsible for ensuring its implementation in practice and for monitoring this over time. They are also responsible for ensuring that appropriate procedures, guidelines or standards as are required to support this are maintained and ownership for these assigned appropriately.

4.2 The RoS Accountable Officer has responsibility for delivery of the enterprise wide implementation of the policy, principles and objectives. The Accountable Officer also approves the governance statement within the RoS Annual Report and Accounts (ARA). The ARA governance statement outlines and evaluates the governance, risk management and internal control arrangements in place during the preceding year. The ARC supports and advises the Accountable Officer in monitoring the corporate governance, risk, value for money and control systems in RoS.

4.3 All Heads of Service are responsible for leading risk management for their services and providing annual certificates of assurance and assurance opinions to the Accountable Officer for the ARA governance statement.

4.4 All RoS colleagues have a responsibility to be aware of risk, and to support and participate in risk management activities led by Heads of Service.

4.5 The RoS ERM service is responsible for the delivery of the integrated ERM framework, including enterprise wide consultancy, training and awareness, on behalf of the Accountable Officer.

5 Approval and review

5.1 This policy will be reviewed annually, unless earlier review is appropriate, by the ARC and RoS Board and approved by EMT.