Registers of Scotland

RoS Board

9 March 2026

Key Risk Register by Exception

Purpose

1. To provide an update on the Key Risk Register (KRR) following Executive Management Team (EMT) and Audit & Risk Committee (ARC) reviews and ongoing Key Risk Owner (KRO) review. This supports the Board in its role of providing strategic advice to the Keeper and in its focus on setting a framework of prudent and effective controls that enables risk to be assessed and managed.

2. To present the reviewed Risk Management and Business Continuity policies following their approval by EMT.

Recommendation

3. That the RoS Board review the KRR updates and advise the Keeper and EMT.

4. That the RoS Board note the reviewed policies as presented in Annex B.

Background

5. The KRR contains risk scenarios that could affect corporate plan objectives, and risk response strategies for these scenarios. It is a live document, reviewed and updated at appropriate intervals by KROs, and reported to EMT each month. A summary of the KRR is submitted to RoS Board and ARC for noting and/or advice.

6. A number of suggestions for the KRR were made during the Corporate Plan and Risk Workshop in January. These are being considered by the Enterprise Risk Management team and KROs.

Key Risk Register

7. We use a reporting by exception approach comprising three elements:

Reporting element	Frequency	Board input required
1. Key Risk Profile	Every Board meeting	Advice on strategic risk exposure
2. New / escalating risks	As relevant	Advice on risk scenario assessments and/or risk responses (i.e. controls)
3. Risk response delays/ controls not delivering anticipated risk response	As relevant	Advice on risk scenario assessments and/or risk responses (i.e. controls)

Element 1 - Key Risk Profile

8. KROs review their risks at a cadence relevant to each risk's current and target scores, progress with route to target and the landscape of factors affecting that risk. A

KRR summary as at the date of this paper is provided at Annex A. The live KRR will be available to RoS Board during the meeting.

Element 2 - New risks / existing risks escalating

9. Key Risk 14: Finance System – Board and ARC suggested we consider broadening the scope of this risk to include HR, and possibly other, legacy systems. Through discussions between the Head of Enterprise Risk Management, Director of People and Operations and the KRO we have concluded that the scope of the risk will remain as is, but that the work being done on a replacement HR system will be noted as this will also look at finance requirements. This will retain the strategic nature of the risk, while ensuring the practical considerations are met. We will give assurance to the Board and ARC by reflecting the practical steps being taken in the controls and route to target for KR14.

10. Key Risks 3 and 4: Operational Capacity and Operational Workforce Productivity – These two risks look at different aspects of capability that are interconnected, and there is duplication and cross referencing between the two. The Head of ERM and KRO have concluded that merging them into a single capability risk will increase the effectiveness of risk management discussions and ensure that all causes, impacts and controls are considered collectively. This change will be reflected in the KRR update provided at the next Board meeting.

Element 3 - Risk response delays/controls not delivering anticipated risk response

11. Nothing to note.

Risk Management and Business Continuity Policy Reviews

12. The Risk Management and Business Continuity policies are reviewed annually. At the 2025 review no changes to the substance of either policy were found to be necessary. Changes to the text made them more concise and added clarity.

13. Both policies were previously mandatory reads for all RoS staff and contingent workers. EMT have agreed that the Business Continuity Policy should only be a mandatory read for C Band and Directors going forward.

Conclusion

14. Updates to the KRR provide evidence and assurance that RoS continues to actively manage and monitor risks and improvement of control environments through route to target activities and mitigating actions to maximise performance and achieve objectives.

15. The Risk Management and Business Continuity policies have been reviewed with no material changes required.

Head of Enterprise Risk Management
Policy and Corporate Directorate
11 February 2026

Annex B: Reviewed Business Continuity and Risk Management Policies

Risk Management policy (changed text in red)

1. **Purpose and scope**
1.1 Risk management involves understanding, analysing and addressing risks to make sure that the organisation achieves its objectives. This policy sets out RoS commitment to managing risk effectively through a consistently applied Risk Management and Assurance Framework.

1.2 The Keeper, RoS Board and the EMT are committed to supporting the benefits of deploying and resourcing an integrated Enterprise Risk Management (ERM) approach to strategic, change and operational risks.

1.3 This policy applies to all RoS activities, including those relating to people, processes, premises, technology, information and supply chain.

2. **Guiding principles**
2.1 We will ensure that risk management at RoS is:

- proportionate and fit for purpose in line with the Scottish Public Finance Manual (SPFM) risk management and internal control guidance
- aligned to the context set by the Corporate Plan
- comprehensive in scope covering all our activities
- embedded across the organisation, including in business planning and decision making
- dynamic to respond to change

3. The Policy
3.1The RoS Risk Management and Assurance Framework reflects the guiding principles and shall be used to operate risk management practices in a standard, consistent and repeatable way across the organisation.

3.2 Risk management will be guided by risk appetite which shall be defined and reviewed by the EMT and documented in the Risk Management and Assurance Framework.

3.3 RoS objectives for ERM are:

- 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 Keeper has overall accountability for risk management at RoS.

4.2 The EMT is responsible for:

- the content of this policy, its approval and review.
- ensuring implementation of this policy in practice and for monitoring this over time.
- ensuring that appropriate procedures, guidelines or standards as are required to support this are maintained and ownership for these assigned appropriately.

setting and communicating risk appetite/s for RoS.4.3 The RoS Accountable Officer (AO) has responsibility for delivery of the enterprise-wide implementation of the policy, principles and objectives. The AO 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.

4.4 The Audit and Risk Committee (ARC) support and advise the AO in monitoring the corporate governance, risk, value for money and control systems in RoS.

4.5 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, as part of the annual Certificates of Assurance exercise. Heads of Service are responsible for ensuring risk management activity informs business continuity arrangements for their services.

4.6 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.

4.7 The RoS Risk and Information Governance function is responsible for the delivery of the integrated risk approach, including enterprise-wide support, training and awareness, on behalf of the AO.

5. **Approval and review**
5.1 This policy will be reviewed annually, unless earlier review is appropriate, by the Information Security and Assurance Group (ISAG) and approved by EMT. A copy will be provided to ARC and RoS Board for noting.

Business Continuity policy (changed text in red)

1. **Purpose and scope**
1.1 This policy sets out the RoS commitment to ensure that previously identified and agreed important business services can continue to operate following an incident that has the potential to disrupt normal service, through business continuity processes and practices.

1.2 This policy applies to all employees and contingent workers.

2. Guiding principles
2.1 RoS, like any other organisation, is exposed to risks that could disrupt or delay critical business functions and/or the delivery of services. Our strategy for continuing business in the event of an incident is to ensure: the safety of all employees, the security of all data; that important tasks continue and the delivery of important business services from predefined locations.

2.2 RoS will align with the International Standard ISO 22301 (Business Continuity management systems – requirements) as the guidance and structure for its Business Continuity activities.

2.3 RoS Business Continuity arrangements will be guided by an understanding of its most important and critical business services ('Important Business Services') which shall be defined by the Executive Management Team (EMT) and kept under review.

3. The policy
3.1 RoS is committed to delivering organisational resilience and recognises the importance of an active and fully supported Business Continuity Programme to ensure the safety, health and continued employment for its employees and contingent workers, quality service delivery for customers and stakeholders, and compliance with Statute and Regulation.

3.2 Each Head of Service in RoS shall prepare, and regularly review, their own comprehensive Business Impact Analysis (BIA) and Business Continuity Plan (BCP) which together contribute towards the overall solution for the Important Business Services of RoS. Plans must be copied to the Enterprise Risk Management team for secure storage.

3.3 Business Continuity Plans shall identify procedures which ensure on-time availability and delivery of required services and must be approved by the relevant Director.

3.4 Each Business Continuity Plan shall be exercised regularly, at a proportionate cadence based on factors such as business criticality of the service, level of change the service has experienced and external factors that could influence the likelihood of an incident. Each exercise shall be reviewed against the relevant BCP and that BCP then updated, if required.

3.5 RoS requires the commitment of each employee and contingent worker, business area and supplier in support of the activities required to protect RoS assets, mission and survivability.

4. Roles and responsibilities

4.1 EMT is responsible for the content of this policy, its approval and review. They are responsible for ensuring its implementation in practice and for monitoring this over time. They are responsible for ensuring that appropriate procedures, guidelines or standards as are required to support this are maintained and ownership for these assigned appropriately. They are responsible for identifying and communicating RoS' Important Business Services.

4.2 The EMT is responsible for ensuring that the commitments given in this policy are met, and that the function is appropriately resourced and accounted for within the wider governance of RoS.

4.3 The Enterprise Risk Management team will ensure that every new and updated BIA and BCP is stored securely in a location that can be accessed appropriately in the event of an incident.

4.4 RoS Digital are responsible for the creation, maintenance and testing of robust Disaster Recovery Plans to ensure that any damage or disruptions to their critical assets can be quickly minimised and that these assets can be restored to normal or near-normal operation as soon as is practicable.

4.5 RoS Communications are responsible for the creation and maintenance of an overall Communications Plan for RoS to use during an incident.

4.6 Heads of Service are responsible for ensuring their business continuity arrangements inform risk management activity for their services.

4.7 All RoS employees and contingent workers have a responsibility to be aware of Business Continuity, and to support and participate in Business Continuity activities led by Heads of Service.

5. Approval and review

5.1 This policy will be reviewed annually, unless earlier review is appropriate, by the Information Security and Assurance Group (ISAG) and approved by EMT.