Registers of Scotland

RoS Board

14 June 2022

Key risk register (KRR) and Business Continuity Policy

Purpose

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

2. The paper provides the board with an opportunity to comment on a draft business continuity policy.

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

Recommendation

4. RoS Board is requested to review the KRR summary at Annex 1 and the risk workshop summary at Annex 2 and advise the Keeper on the update.

5. RoS Board is requested to review the draft business continuity policy at Annex 3 and provide advice to EMT in order to complete the review, approval and adoption of the policy.

Background

6. 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.

7. RoS has established a business continuity (BC) taskforce to enhance its BC capability, respond to ongoing organisational change and aspirations, and to provide a foundation for realising a state of 'organisational resilience'.

8. Enhancing BC governance arrangements are integral to this work. Best practice recommends the adoption of a business continuity policy as a key component of BC governance arrangements.

9. The draft policy and RoS Policy Checklist is at Annex 3.

Key risk register (KRR)

10. The paper adopts a 'reporting by exception' approach 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 the KRR
2. New/developing risks	As relevant	Advice on how risks have been assessed in terms of 'causes - 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 - scenario – impacts' and the risk response (i.e. controls)

Key risk register – reporting element 1

11. 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 June 2022 meeting.

12. The annual risk workshop was delivered on 24 May 2022. The workshop concluded our risk exposure continues to be captured by the set of risks previously identified in KRR 2021-26. A summary of proposed changes to key risk scenarios for KRR 2022-27 is included at Annex 2.

Key risk register – reporting element 2

13. The annual risk workshop summary at Annex 2 provides details of potential new / developing risks.

Key risk register – reporting element 3

14. 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'.

15. The criticality and interdependence of our responses to Key Risks 3 Operational Capacity and 7 People & Change is noted in Annex 2. EMT intend to focus on both risks in 2022-23, with risk reviews in the coming months re-visiting the planned routes to target for each risk. Key considerations will include whether control interventions are sufficient to fully address each risk, the timing and sequence of interventions, and suitable means of assurance to demonstrate the effectiveness of our interventions.

16. Risk and Information Governance (RIG) service will refine the updated draft KRR 2022-2027 for final review at planned EMT, RoS Board and ARC meetings. The following meetings are currently scheduled:

a. EMT CG monthly KRR Reviews 26 May, 24 June and 28 July 2022

b. ARC KRR Assurance Framework Review 9 August 2022

c. RoS Board KRR and Assurance Framework Review 14 June, 13-14 September 2022

17. When final approval of a 'live' KRR 2022-2027 is complete, RIG will draft an updated Assurance Framework 2022-2027 for ARC, RoS Board and EMT ongoing review and oversight.

Business Continuity

18. The policy has been informed by a range of industry standards, including the Business Continuity Institute's "Good Practice Guide" (link) and the BC ISO-standard (ISO22301). Our BC Lead (recruited externally to add subject matter expertise based on significant experience of implementing BC in a range of organisations), has contributed to the policy and helped tailor best practice to the RoS context.

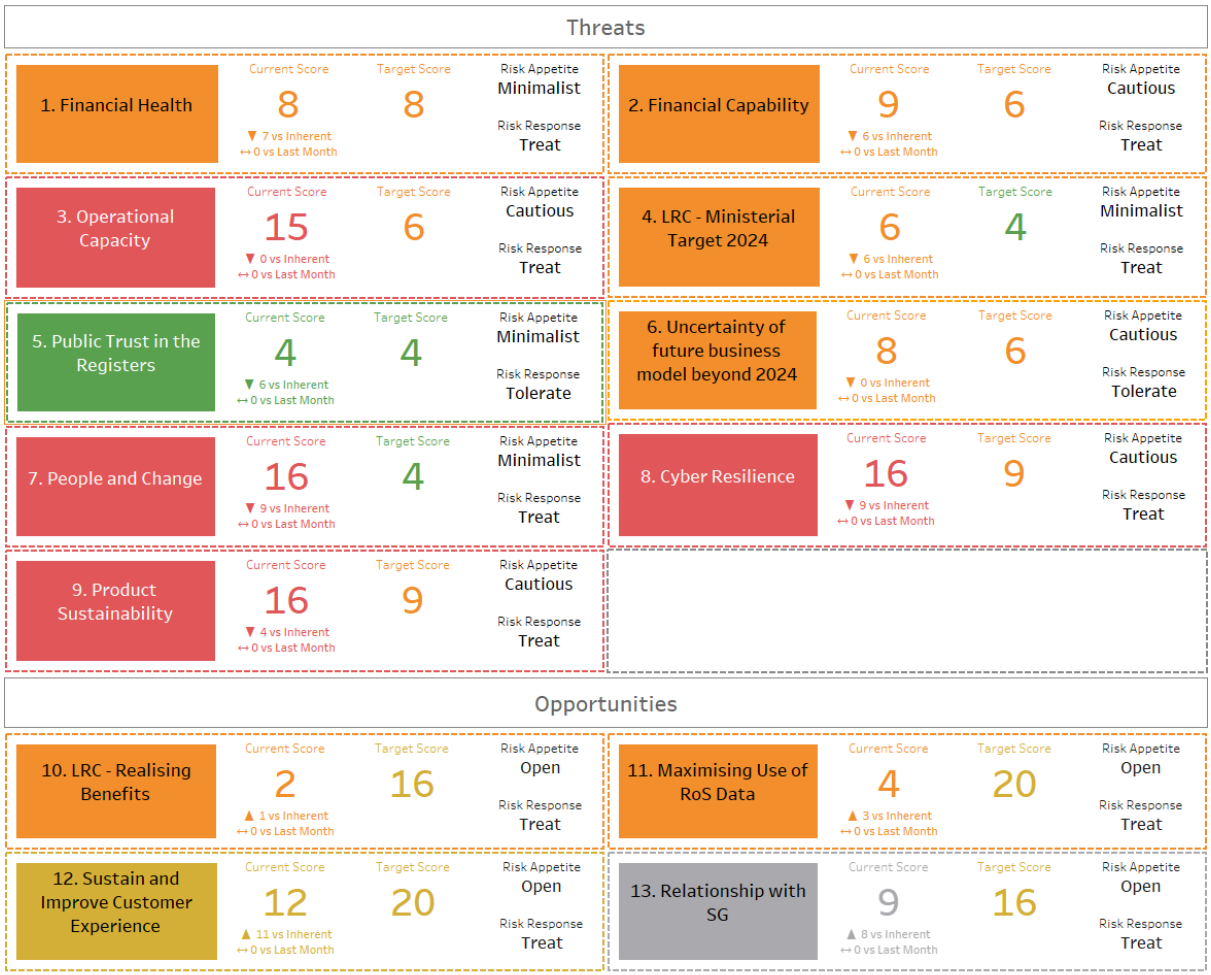
19. The policy has been reviewed by EMT, ARC and PCS. Following review by the board, EMT will consider any board comments and complete final approval of the policy at the June EMT CG meeting, with publication on RoS intranet to follow.

Conclusion

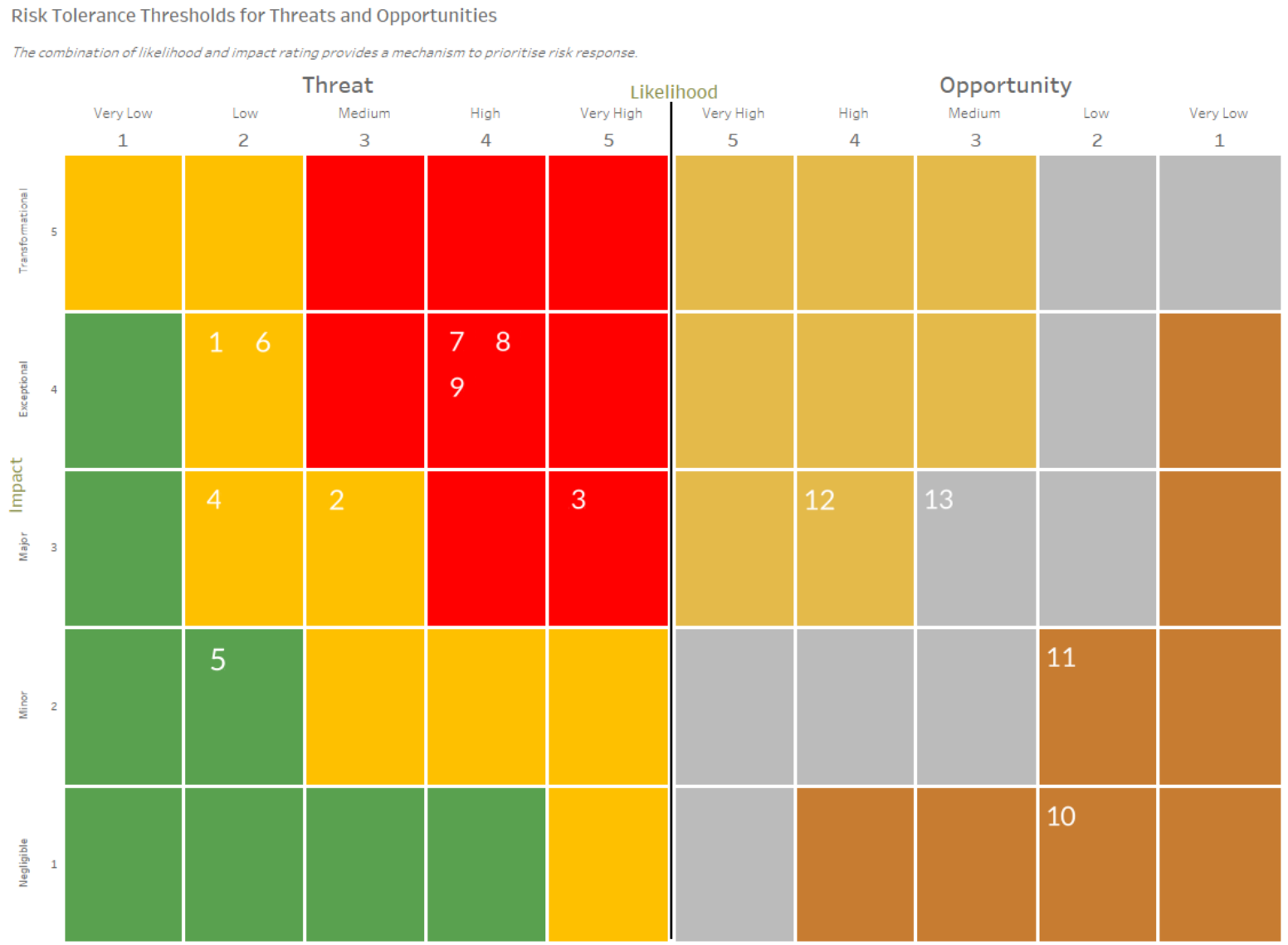
1. RoS Board to review the KRR update and draft business continuity policy, Annexes 1, 2 and 3, and consider the background, topic matter and recommendations in this paper for advice to the Keeper and EMT.

Head of Enterprise Risk Management
Corporate
27 May 2022

Annex 1a Key Risk Register infographic



Annex 1b Key Risk Register matrix



Annex 3 Draft business continuity policy and policy checklist

Business Continuity Policy

Author	Business Continuity and Organisational Resilience Lead		
Reviewed	Head of Enterprise Risk Management		
Cleared	Corporate Services Director		
Approval	EMT	Approval Date	24 June 2022
Policy Version	DRAFT v01		
Review Responsibility	EMT	Review Date	24 June 2023
Suitable for Publication	Y		
Contact:	rossecretariat@ros.gov.uk		

1 Purpose and Scope

1.1 This policy sets out the Registers of Scotland (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 the normal service provided.

1.2 This policy applies to all employees and contingent workers.

2 Guiding Principles

2.1 RoS is committed to providing the best possible experience to its customers and the best possible relationships with employees, contingent workers and suppliers. To ensure the consistent availability and delivery of services provided, RoS has developed this Business Continuity Policy in support of our Business Continuity Programme and overall organisational resilience.

2.2 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.

3 The Policy

3.1 RoS is committed to delivering organisational resilience.

3.2 Each Head of Service in RoS shall prepare and review their own comprehensive Business Impact Analysis (BIA) at least every 6 months and their Business Continuity Plan (BCP) at least annually: which both together contribute towards the overall solution for the Important Business Services of RoS.

3.3 When a Business Continuity Plan is completed, approved by the associated Director and implemented, each plan shall identify procedures which ensure on-time availability and delivery of required services.
3.4 Each Business Continuity Plan shall be exercised as a minimum on an annual basis to ensure compliance with this Business Continuity Policy. Each exercise shall be reviewed against the relevant BCP and that BCP then updated, if required.
3.5 RoS will align with the International Standard ISO 22301 (Business Continuity management systems – requirements) as the guidance and structure for its Business Continuity activities.
3.6 RoS 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.
3.7 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 Executive Management Team (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.
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 Every BIA and BCP update shall be copied to the Enterprise Risk Management Team and the Chair of the Business Continuity Steering Group (to be stored securely).
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 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 and approved by EMT on an annual basis, unless earlier review is appropriate.

Annex A – Definitions of Key Terms

Business Continuity Plan (BCP)
A documented collection of procedures and information that is developed, compiled, and maintained in readiness for use in an incident to enable an organisation to continue to deliver its critical products and services at an acceptable predefined level.

OR - A documented plan that details how an individual organisation will ensure it can continue to perform its essential functions during a wide range of events that impact normal operations.

Business Continuity Policy
The key document that sets out the scope and governance of the BCM programme and reflects the reasons why it is being implemented.

Business Continuity Programme
Ongoing management and governance process supported by Top Management and appropriately resourced to implement and maintain Business Continuity Management.

Business Continuity Management System (BCMS)
Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity. ISO Editor's Note: The management system includes organizational structure, policies, planning activities, responsibilities, procedures, processes and resources.

Business Continuity Taskforce Steering Group
The Business Continuity Taskforce Steering Group is an interdisciplinary team to ensure the RoS Business Continuity Taskforce aligns to corporate strategy and objectives, is maturing, making forward progress towards annual goals, and furthermore, helps to raise the profile and awareness of Business Continuity Management.

Business Impact Analysis (BIA)
Process of analysing activities and the effect that a business disruption might have on them.

Contingency Plan
A plan used by an organisation or business unit to respond to a specific systems failure or disruption of operations.

Disaster Recovery (DR)
The technical aspect of Business Continuity. The collection of resources and activities to re-establish information technology services (including components such as infrastructure, telecommunications, systems, applications and data) at an alternate site following a disruption of IT services. Disaster recovery includes

subsequent resumption and restoration of those operations at a more permanent site.

Disaster Recovery Plan
A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.

Embedding Business Continuity
The Management Practice within the BCM Lifecycle that continually seeks to integrate Business Continuity into day-today activities and organizational culture.

Important Business Service
A service provided by RoS, or on behalf of RoS, to customers (both external and internal) which, if disrupted, could cause intolerable levels of harm to any one or more RoS customers.

Incident
An event that has the potential to cause interruption, disruption, loss, emergency, crisis, disaster, or catastrophe.

Incident Management Plan
A document that helps an organisation return to normal as quickly as possible following an unplanned event.

Information Security Continuity
A term used within ISO 27001 to describe the process for ensuring confidentiality, integrity and availability of data is maintained in the event of an incident, i.e. the focus is on ensuring information security functions are maintained, not that Services are maintained.

Intolerable Harm
Something from which customers cannot easily recover, e.g. where a firm is unable to put a client back into a correct financial position, post-disruption, or where there have been serious non-financial impacts that cannot be effectively remedied.

Maximum Tolerable Period of Disruption (MTPD)
The time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing and activity, to become unacceptable.

Operational Resilience
Ability of an organization, staff, system, telecommunications network, activity or process to absorb the impact of a business interruption, disruption or loss and continue to provide an acceptable level of service.

Organisational Resilience
The ability of an organisation to anticipate, prepare for, and respond and adapt to incremental change and sudden disruptions in order to survive and prosper.

OR – The ability of an organisation to absorb and adapt in a changing environment.

Recovery Point Objective (RPO)
Point to which information used by an activity must be restored to enable the activity to operate on resumption. Note: Can also be referred to as “maximum data loss”.

Recovery Time Objective (RTO)
Time goal for the restoration and recovery of functions or resources based on the acceptable down time and acceptable level of performance in case of a disruption of operations.

Resilience
The ability to prepare for and adapt to changing conditions and recover rapidly from operational disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.