Registers of Scotland
ros.gov.uk

Security and Information Assurance

Information Risk Policy

Registers of Scotland
Departmental Security Group
Policies and Procedures

Department	Security and Information Assurance (SIA)
Topic	Information Risk Policy
Number	SIA10
Date	19 Jun 2015

Information Risk Policy

Contents

Purpose

1. This document sets out RoS Registers of Scotland (RoS) Information Risk Policy and builds on the RoS Information Security Policy.

2. RoS Information Risk Policy defines how RoS and its delivery partners, delivery chains and 3rd party suppliers[1] processing or handling information on RoS behalf will manage Information Risk and how its effectiveness will be assessed. The policy supports RoS's strategic aims and objectives and will enable individuals throughout the delivery chain to identify an acceptable level of risk, beyond which escalation of risk management decisions is always necessary. The policy fits within RoS's overall business risk framework.

RoS commitment

3. The RoS Board and Executive Management Team fully support the requirement to establish and maintain an effective Information Risk Strategy and Management Framework covering the whole RoS operation, including its delivery partners, delivery chains and 3rd party suppliers, as a means of reducing Information Risk and enabling the effective use of information for the public benefit.

Information

4. Information takes many forms and can be stored physically or electronically, transmitted across networks or telephone lines, sent by fax, printed as hardcopy or written on paper and spoken in conversations.

The Threat

5. Information is a very valuable asset. Without it RoS, like most other organisations, would be unable to function. The integrity of RoS's information is vital, particularly in respect to the statutory registers that the Keeper of the Registers of Scotland administers.

6. RoS are duty bound to protect deeds and other documents belonging to other parties which are submitted to RoS from loss or compromise.

Information Risk Management strategy

7. RoS Information Risk Management will align with in respect to our risk appetite (as defined in our risk appetite statement), risk tolerance and the sharing of information.

8. RoS Information Risk Management will align with the security controls in ISO/IEC 27002:2013[2] and other pertinent best practice.

[1] The definition of these parties are narrated in Appendix 1.

[2] BS ISO/IEC 27002:2013 is the international code of practice for information management.

Information Risk management structure

9. RoS will establish and maintain an Information Risk management structure with specific roles and responsibilities, including the procedures for approving deviations from the policy.

10. The RoS Senior Information Risk Owner (SIRO) owns the Information Risk Policy and risk assessment. The SIRO acts as an advocate for Information Risk on the RoS Board and in internal discussions, and as the Accountable Officer for RoS signs the Statement on Internal Controls relating to Information Risk included in the Annual Accounts.

11. The SIRO is responsible for developing and implementing the Information Risk Policy and for reviewing it regularly to ensure that it remains appropriate to the business objectives and the risk environment. The Information Risk Policy will be published and communicated in a manner that is relevant, accessible and understandable to all employees and relevant third parties.

12. RoS has appointed dedicated Information Asset Owners (IAOs) to be responsible and accountable for all its information assets[3].

13. IAOs have responsibility for setting out the rules and controls to ensure confidentiality, integrity and availability for their information assets.

14. IAOs must advise the SIRO immediately if their information assets are compromised.

Information Risk Appetite

15. The Executive Management Team is responsible for setting the RoS Information Risk appetite.

Information Asset Register

16. RoS will maintain an Information Asset Register covering all RoS information assets, including those hosted on third party services.

17. IAOs are responsible for reviewing the Information Asset Register, at least every 3 months, and ensuring that it is current and accurate.

18. IAOs will ensure that members of staff and other relevant parties, with access to or involved in processing and / or handling RoS information assets are identified in the Information Asset Register.

19. IAOs are responsible for ensuring that information whose release or loss could cause harm or distress to individuals is recorded in the Information Asset Register.

20. The Security and Information Assurance (SIA) team will be custodian of the Information Asset Register. They will be assisted by the Directorate Area Information Managers (AIMs).

[3] RoS definition of an information asset is a separately describable set of data or information which is of sufficient value to the business that will be retained for a period of time.

Information Risk Register

21. RoS will establish and maintain an Information Risk Register which will form part of the Corporate Risk Register and will be owned by the SIRO. The Risk Manager will be custodian of this register.

Delivery partners, 3rd party suppliers and delivery chains

22. IAOs are responsible for identifying all RoS delivery partners, 3rd party suppliers and delivery chains and documenting what RoS information assets they process and / or handle.

RoS Information Sharing

23. IAOs will consider on an annual basis how better use could be made of their information assets and take effective action to maximise the public benefit derived from the information for which they are responsible.

24. Where information is shared by one IAO but owned by another IAO (for example Commercial Services sharing Registration material with customers). The approval of the accountable IAO (i.e. Registration in the example above) will be obtained.

25. IAOs will ensure that records are maintained of what information is shared with other organisations and the extent of the detail that is shared.

26. IAOs will be responsible for ensuring that Information Risk Assessments have been agreed with organisations that they share data with.

Information Risk Assessment and Reduction

27. IAOs will (a) review the adequacy of the information management, practices and procedures and the risks that threaten the confidentiality, integrity and availability of their information assets and (b) ensure that their reviews also examine forthcoming changes in services and technology, and any associated threats. IAOs will provide the SIRO with quarterly assurances that they have done so; that the security measures they have in place are effective and show whether there is any increase or decrease in threat. The SIRO will provide this detail to the Audit Committee.

28. The IAOs will carry out their quarterly assurances using the agreed RoS template form to achieve a consistent approach across RoS.

29. The SIA team are responsible for monitoring that technical risk assessments are carried out on ICT systems processing RoS information assets.

30. The SIRO is responsible for ensuring that an annual Information Risk assessment is completed which includes an assessment of the effectiveness of the overarching Information Risk Policy.

31. Where the delivery chain involves the handling of information relating to 100,000 or more identifiable individuals, RoS will engage independent security experts to carry out IT health checks (penetration testing) on the appropriate ICT systems.

32. Where risk assessments or IT health checks identify threats or risks to information then RoS will apply promptly measures to eliminate or reduce the threat or risk.

Culture and awareness

33. RoS will provide and maintain an Information Risk awareness programme to promote a culture in RoS to ensure that information is valued, protected and used for the public good.

34. RoS will introduce measures to reward positive approaches to information risk and penalise negative activity.

35. RoS will establish a programme where all RoS staff must successfully during induction and regularly undergo Information Risk awareness training. This will include the corporate and individual consequences of failure to apply the RoS policies and practices, including disciplinary measures that will be taken in the event of failure to adopt RoS policies and practices.

Clearance

36. IAOs are responsible for identifying which staff roles require additional clearance over and above the RoS baseline clearance.

37. IAOs are responsible for checking that appropriate clearance checks have been carried out on individuals of delivery partners, 3rd party suppliers and delivery chains who process and / or handle their information assets.

Information Risk incident management

38. Information Risk incidents will be managed in line with the RoS Information Incident Response management procedures and guidance.

39. RoS will establish mechanisms to allow individuals to directly highlight concerns they may have about Information Risk to the attention of Senior Management or the Audit Committee.

RoS information outside RoS premises

40. RoS will carry out risk assessments for all cases where information is taken outside RoS premises.

41. RoS will develop and maintain Remote / Agile working policies and guidance.

Sensitive / business critical information

42. It will be RoS policy to accredit formally to the Government standard all systems that process sensitive and / or business critical information and re-accredit when systems undergo significant change or at least every five years.

43. RoS will establish and maintain both technical and procedural controls to reduce the risk of information loss, both inside and outside RoS premises.

44. Where there is a robust business requirement to take sensitive / business critical material outside RoS premises, then IAOs will formally consider the risk and only

approve where the necessary protective controls have been established for individuals to do this safely.

Monitoring compliance

45. It is the responsibility of all RoS managers to monitor that their staff are adopting our Information Risk policies and practices. IAOs will periodically arrange for inspections, reviews (internal and external), monitoring and audit to check compliance.

46. It is the responsibility of the IAOs to monitor periodically that delivery partners, 3rd party suppliers and delivery chains processing and / or handling their information assets, are aware of and comply with RoS policies and procedures.

47. IAOs will be responsible for ensuring that any required Information Risk action carried out on their behalf has been completed successfully and where it has not, ensure that remedial action is taken.

48. RoS will periodically arrange for independent reviews to be carried out of the effectiveness of the RoS Information Risk Management framework.

Transparency

49. RoS will publish and maintain an Information Charter on their website.

50. RoS will conduct Privacy Impact Assessments when changes are made to the processing of information so that they can be considered as part of the Information Risk aspects of Gateway Reviews or while going through the accreditation process. The Programme Manager will ensure that that Privacy Impact Assessments are considered by the Senior Responsible Owners involved in the RoS Change Programme.

Appendix 1 – Definition of delivery partners, chains & 3rd party suppliers

51. This definition has been copied from a Cabinet Office publication.

Delivery Partner

Any organisation with whom the Department either has an exchange of information and uses that information to carry out a business role, or delivers a service on behalf of Government.

A Delivery Partner may be:

- another Government Department;
- a non-ministerial Government Department;
- an Executive Agency;
- a Non Departmental Public Body (NDPB);
- devolved administrations;
- overseas government departments;
- a wider public sector body, e.g. regional or local government, emergency services, Higher Education Institutes;
- a private sector organisation, e.g. business consultancy, public corporations; or
- a third sector organisation, e.g. charitable trust.

Major Delivery Partner

These are organisations with which a Department has a significant exchange of protected personal or business critical information, or holds such information in their own right, and where the loss or compromise of that information would impact appreciably on individuals or on the Department.

A Major Delivery Partner could be one which:

- handles large quantities (as defined by the HMG Data Handling Review) of protected personal, protectively marked or business critical information on behalf of the Department and where any loss of that data would cause distress or damage to individuals, or;
- where any data loss might be indicative of a systemic failure between the Department and its Delivery Partner; or
- provides services to the Department the loss of which would severely disrupt the delivery of the Department's business objectives, or

- where any data or service loss would result in the Department involved, and/or the Government, suffering reputational damage impacting on their ability to maintain the trust of the citizen and business.

3rd Party Supplier

A 3rd Party Supplier is a commercial entity contracted to supply ICT and related non-ICT services to government and includes their own suppliers and information/service exchange arrangements.

Delivery Chain

The information exchange flow between Delivery Partners, and where appropriate 3rd party suppliers. A Delivery Chain may be composed of several Delivery/Major Delivery Partners in order to process information and convey a service or information to the citizen. Delivery Chains are categorised as information holdings and exchanges between the Department and one or more of the following:

- its third party suppliers, for example IT service providers (i.e. where there is a contract in place between the Department and the supplier related to the management of or an exchange of information; it is the responsibility of the Department to provide assurance that protected personal and business critical data is handled appropriately by its suppliers.);
- Large or sensitive Agencies, NDPBs, and other key near-to-government bodies. (A useful definition being those organisations that are included in the Resource Accounts of the Department, e.g. Identity & Passport Service (HO), Jobcentre Plus (DWP), the General Teaching Council (DCSF);
- Other delivery bodies including but not limited to:
    - Agencies, NDPBs, and other near-to-government bodies not covered in the Resource Accounts
    - Regional and Local Government organisations
    - “Blue Light” organisations, i.e. emergency services
    - The third sector
    - Other non-government organisations (NGOs)