RoS Information Assurance handbook

Contents

1. Ten golden tips

Please find below some useful tips that all staff can use to ensure our information is handled appropriately.

In the office

1. Never access information unless it is part of your job and you have a business need to do so.
2. Observe a clear desk policy and always 'lock' your computer before leaving your desk.
3. Choose your password carefully and never let anyone else know it.
4. Challenge anybody in your building who is not wearing an appropriate security pass.
5. Always make sure you know what classification the information should have and stick to the rules for that level of protection.

On the move

6. Never take sensitive information out of the office without authority. Never use removable media unless it is business critical that you do so.
7. Keep your laptop, Blackberry, phone and any official papers secure at all times.
8. When working outside ensure that you are not overheard and that information cannot be seen by others and do not use public Wi-Fi or Wi-Fi in a hotel to access work information at anytime.

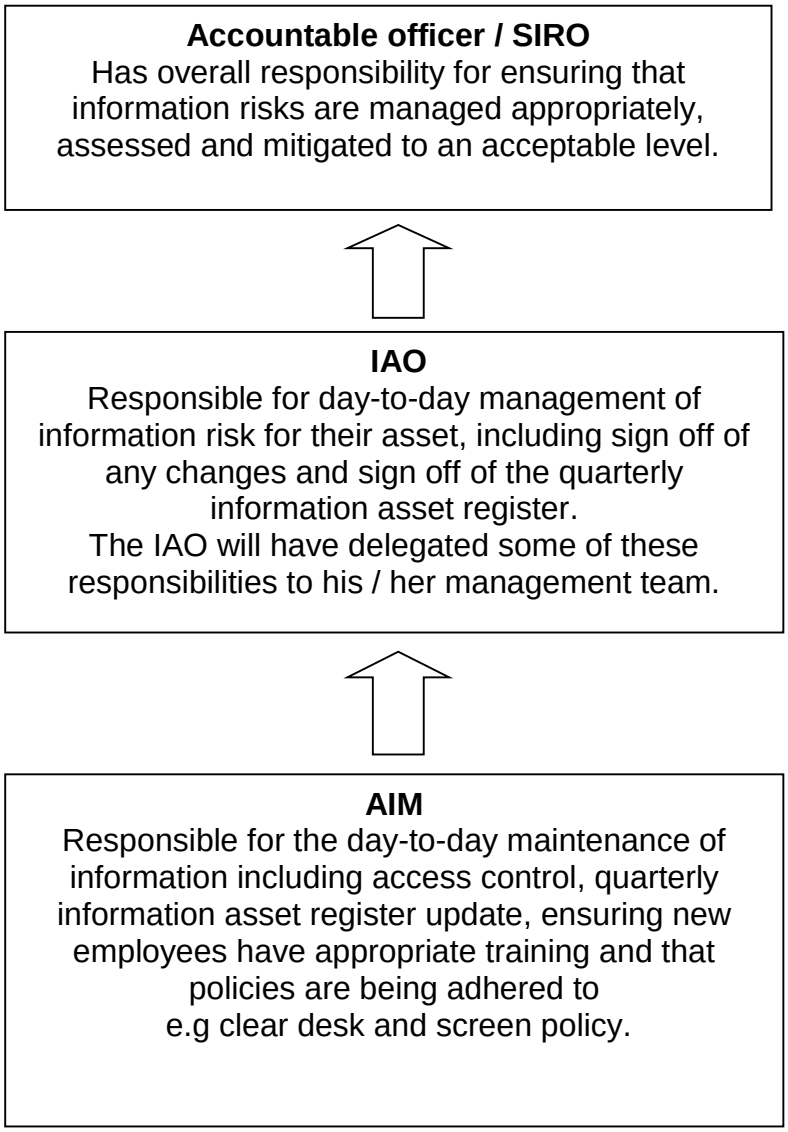
Sharing data

9. Never give out sensitive information over the phone or in any other way unless you are absolutely sure who you are giving it to and that they are entitled to that data.
10. When emailing, ensure you have the correct address for your recipient and that there is a business requirement to share that information with them. There are set procedures for who and how you can email per specific classification. Make sure you follow these accordingly.

2. Introduction

The HMG security policy framework (SPF) states that organisations should appoint and train information asset owners (IAO) for each of their information assets. The role was created following the government's data handling review in 2008. An IAO is appointed by, and reports to, the senior information risk owner (SIRO). Their role is to protect and manage information held in HMG, and ensure that its value to the organisation is fully exploited.

This handbook will help you understand your role and responsibilities within Registers of Scotland (RoS), the chain of governance (including where you fit in), and the skills you need to be an effective IAO. Please see reporting chain below:



Who should hold the role of information asset owner?

IAOs are senior/responsible individuals working in a relevant business area. Their role is to understand what information is held, what is added and what is removed, how information is moved and who has access and why. As a result they are able to understand and address risks to the information, ensure that information is fully used within the law for the public good and provide written input to the SIROs annually on the security and use of their assets.

As an IAO you will be responsible for an information asset in terms of:

- identifying risks associated with the information asset;
- managing and operating the asset in compliance with policies and standards; and;
- ensuring controls manage all risks appropriately

The role you perform is flexible and may be implemented differently in organisations. Most IAOs will perform the role in addition to existing duties, and for some, responsibilities may be shared between many individuals. It is more important that the relevant responsibilities of the role of IAO are performed; not necessarily who does them.

3. Training

IAO skills development journey

- Civil service learning
    - Responsible for information – information asset owner (IAO) including government security classifications
- Familiar with the detail in this handbook
- Appropriate risk management training
- Additional external training as determined by the SIRO

4. Identifying information assets

4.1. Definition of an information asset

An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively.

An asset can be a single significant document or a set of related data, documents or files; it can be shared or be confined to a specified purpose or organisational unit.

How to identify an information asset

To determine whether a body of information should be considered an information asset, begin by asking the following questions:

Does it have a value to the organisation?
• will it cost money to re-acquire the information? Would there be legal, reputational or financial repercussions if you couldn't produce the information on request or this information was made public? Would it have an effect on operational efficiency if you could not access the information easily? Would there be consequences of not having this information?
Does the group of information have a specific content?
• do you understand what it is and what it is for? Does it include all the content associated with the information?
Does the information have a manageable lifecycle?
• were all the components created for a common purpose? Will they be disposed of in the same way and according to the same rules?
Is there a risk associated with the information?
• is there a risk of losing the information, or that it is inaccurate, someone may try and tamper with it, or that a risk could arise from inappropriate disclosure?

If the answer is **yes** to these questions, then your information should be registered in your information asset register.

Grouping information assets

- Information assets should be grouped and considered depending on their business needs, not on their technology requirements. Each asset may contain individual items that need different technology solutions to address the same business need.
- Where an asset comprises a collection of information with a range of different sensitivities or security classifications, the highest security level present in the collection will be ascribed to that asset to identify the minimum security level required in practice.

Examples of information assets:

- a database of contacts - All the pieces of information within the asset will have similar risks associated with privacy and storage of personal information so each entry does not need to be treated individually and can therefore be considered one information asset
- all files associated with a specific project - This might include spreadsheets, documents, images, emails to and from project staff and any other form of records. All the individual items can be gathered together and treated as one single asset as they have similar definable content, and the same value, business risk and lifecycle.
- a database of related information such as an HR system that is shared across the organisation
- a set of statistical data to inform returns (such as attendance spreadsheets)
- paper files or other physical media held at a location for a specified purpose
- a single document with specific and significant management conditions e.g. one containing personal and sensitive data
- a collection of documents on a subject for a specified purpose
- a storage file with significant management conditions, such as a casework file containing personal and sensitive data restricted to casework staff
- a set of general administration files where you have “lead responsibility”
- source code which RoS has written for an IT system

Corporate assets

A corporate asset is a type of information asset that requires additional considerations. They can be defined as assets that have broad access across the business and are utilised to achieve multiple differing objectives, for example; our public registers.

The following are examples of additional considerations for corporate assets:

- it is recommended that the IAO ensures that risks to the asset are being managed at the appropriate level
- responsibility for various aspects of managing this asset, for example maintaining user lists may need to be delegated by the IAO to responsible individuals

Information systems

It is important to recognise the difference between an information system and an information asset. An information system may contain single or multiple information assets. For example; a computer network (an information system) can contain multiple databases (information assets).

Third parties

Assets that are hosted externally by a third party are still under the ownership and management of the organisation and therefore require an IAO within the organisation.

4.2. Information asset register

An information asset register (IAR), which lists our information assets alongside their associated owners (IAOs) must be maintained. Within RoS the IAO is required to submit a quarterly return covering inter alia, their information asset register. The area information manager (AIM) will collate the information every three months and send to the IAO to be signed off. This information is then presented to the information assurance group (IAG) at their quarterly meeting.

The IAR is a list of personal or otherwise sensitive information assets held by your organisation. It should also include assets that are business critical or required for business continuity. Examples of the type of information held on an IAR are:

- classification
- IAO details
- format
- description and purpose of asset
- access
- retention and disposal schedule
- storage

It is essential that IARs are up to date and accurately reflect the information assets held by organisations. As an IAO, it is important that you understand your organisation's processes for recording changes relating to information assets.

4.3. Removing assets from the IAR

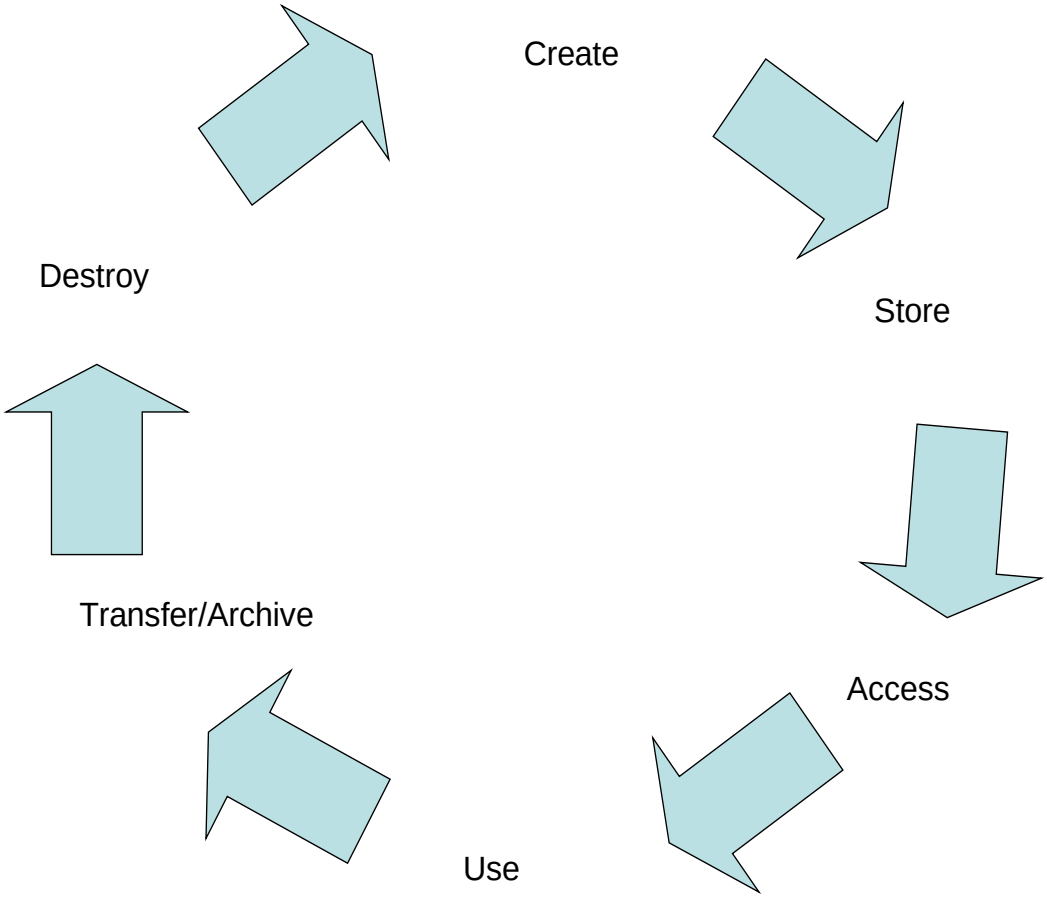
An information asset may be superseded by other work, or have come to the end of its lifecycle. In such cases the IAO will need to determine whether the information asset still needs to be kept and if so, may want the IAR updated to highlight that the information asset carries a lower level risk than before. Alternatively, it could be removed from the IAR as there is no longer a business need for it or it has been destroyed.

For assets that are archived it is important that an IAO remains in place and that they still maintain responsibility for that asset.

Information lifecycle

The information lifecycle is the combination of people processes and technology that enables business information to be effectively and cost efficiently managed.

The lifecycle has been designed to facilitate easy access to all stages of the life of the information – from its creation to its disposal.



5. Managing your information assets

IAOs must ensure that any information assets they are responsible for are properly protected and their value to the organisation fully realised. Aspects of the role may require IAOs to take direct action whilst some activities are simply to assure that action is being taken by others.

5.1. The IAO terms of reference

The following tables expand on the responsibilities of an IAO (some of the day-to-day activities the IAO may have devolved to others):

Know what information the asset holds, what enters and leaves it and why
▪ understand and address risks to your information assets ▪ know who has access to your information assets and why, and monitor use ▪ understand whether a delivery partner or supplier has a dependency on your information to deliver a service and how they use and protect that information ▪ approve and minimise transfers while achieving the business purpose ▪ approve arrangements so that information from the asset put onto removable media such as disks or laptops is minimised and protected appropriately with approved encryption methods where required ▪ approve the disposal mechanisms for paper or electronic records from the asset, in accordance with organisational policy ▪ make sure your information assets are fully used for the public good, including responding to access requests and alignment with the transparency agenda. This includes actively considering whether public protection/services could be enhanced through greater access to the information assets that you're responsible for.

Supporting actions

Document your understanding of the information assets:

- what the assets are – what they cover, their content, what's sensitive and/or protectively marked and what personal data you're responsible for
- the value of your information assets to the business – now and in the future. How important are they, and why? What would be the impact of losing or mishandling them? As part of this process consider the benefits of increasing access or of information re-use
- your usability requirements for those assets – who needs to be able to find them
- what retention and disposal schedules you need
- keep a record of all staff and contractors with access to information containing personal data. Ensure a process is in place to remove that access as soon as it is no longer required
- manage agreements on sharing personal and sensitive information between organisations

Know who has access and why, ensure use is monitored and compliant with policy

- understand your organisation's policy on use of the information
- be aware of and understand relevant statutory requirements with regard to handling information
- check that access provided is the minimum necessary to achieve the business purpose
- consider requests for access to information from other business users, and maintain log of requests and decisions
- report breaches promptly in accordance with your organisations procedures

Supporting actions

- get assurance from others: You don't have to monitor access directly but you do need assurance that it is being done.
- get assurance from your IT organisation that access rights to IT systems are limited to the appropriate people.

Identify, understand, manage, report and record risks to the business in relation to your asset(s), and provide assurance to the SIRO

- contribute to the implementation of the information risk management policy in your business area
- contribute to the organisation's risk assessment
- provide written assessments to the SIRO on the use and security of the information assets you are responsible for and the information you hold
- make the case where necessary for new investment to secure the asset

Supporting actions

Risk Management

- read your organisations risk management and information risk management polices
- attend IAO risk management training - this should indicate where losses of confidentiality, integrity and availability are likely to have the most critical impact on your business and where the greatest proportion of your mitigation should be focused
- if operating under an exemption/variation to policy, ensure that this still applies as they are usually granted by the SIRO for a limited time period
- databases: is it easy to know who has access, or to identify what is personal/sensitive data? Is the management of databases consistent? If your protocols for protecting personal data differ across databases, why is this?
- inappropriate access to shared drives: who has access to information assets on shared drives and why? Do you know what sensitive personal/sensitive data is held there? Do you have arrangements for protecting it?
- are access controls being applied properly and consistently to information assets on shared drives?
- does your email have a security classification? Where are emails stored and how are they protected?

Ensure the asset is fully used for the public good, including responding to requests for access from others

- ensure that you are able to use information assets as appropriate to comply with public data and transparency requirements
- ensure decisions on access are taken in accordance with standards of good practice and the policies of your organisation
- consider whether better use of the information is possible or where it is no longer required
- manage and approve agreements on sharing personal information between organisations and ensure access decisions are taken accordingly
- receive, log and control requests from others for access

Supporting actions

- review the assets for which you are responsible to see whether they are suitable for release to increase the organisation's transparency
- where appropriate, provide advice to others in your business areas on the suitability of the release of datasets

Lead and foster a culture that values, protects and uses information for the success of the organisation and the benefit of the public

- through your behaviours, demonstrate commitment to the importance of good information management
- lead by example and champion cultural change activities, for example by encouraging your colleagues to complete the mandatory e-learning training
- help your colleagues to be aware of their responsibilities regarding the management of information
- help ensure appropriate action is taken in cases of breaches or non-compliance
- help to foster an environment where information assurance concerns can be raised and discussed openly
- attend training – as mandated by your organisation
- ensure the handling of your information assets complies with the Data Protection Act (1998) and aligns with the requirements of the transparency agenda

Supporting actions

- participate in and contribute to activities of the IAO community, identifying best practice and opportunities for continuous improvement
- make sure that people who use your information assets understand the rules and are aware of the consequences of non compliance. Explore using line management responsibilities – appraisal and objective setting – to monitor this
- set up a lessons learnt log so if things go wrong you can learn from them and ensure policies and practices are changed
- exchange ideas and network with other IAOs

6. Risk management

IAOs should familiarise themselves with the risk management practices of their organisations, specifically how to identify, understand, manage, report and record risks. Understanding your organisation's risk appetite is also important, as it will help you to align any risk-based decisions you make regarding assets for which you are responsible, with the wider organisational approach.

An IAO's role is a key element in an organisations efforts to manage information risk. SIROs will look to IAOs for the day-to-day management of information risk and to highlight systematic risks which the organisation may need to address.

For your purposes risk appetite can be defined as; a threshold, set by your organisation, relating to the level of risk it considers acceptable and which should not be exceeded, unless approved by your SIRO.

Definition of information risk management:

The culture, processes and structures that are in place to effectively manage any potential unwanted effects or events (risks), which may negatively impact your information assets or their use.

The complete process of identifying, controlling and mitigating risks includes;

- risk assessment (see below)
- cost benefit analysis, and
- the selection, implementation, testing and security evaluation of controls

A complete risk assessment considers both the effectiveness and efficiency of the controls selected (see above), any relevant constraints laid down in policy, regulation or law and must take into account any impact on achievement of business objectives.

Risk assessment

Risk = threat x vulnerability x likelihood x impact

Risk assessment tends to be used as a short-hand term to cover processes to identify and evaluate:

Threat – what can go wrong?

Risk – what is the chance of it happening?

Risk assessment – what would be the consequences/impact?

Risk management – what can be done about it?

6.1. Potential risks to your assets

Below are some examples of potential risks and threats to your information assets.

Risk category	Example of risk	Example of threat
Governance and culture	• lack of effective governance arrangements, comprehensive oversight and control • lack of proper procedures for handling incidents, including identifying and acting on lessons learned • third parties letting you down (suppliers do not apply the same standards of information security as we apply ourselves)	• new business services not taking risk information into account • culture that does not recognise the importance of protecting information at the same time as looking for opportunities to share and exploit it
Information management and information integrity	• critical information is wrongly destroyed, not kept or cannot be found when needed • information becomes unreadable due to technical obsolescence • information is lost	• lack of basic records management disciplines or non-compliance with agreed processes • inaccurate information • staff not following security policy or guidance with information in their care.
The human dimension	• despite having procedures and rules, staff, acting in error, do the wrong thing • inappropriate disclosure of information	• despite having procedures and rules, staff do the wrong thing deliberately (insider threat) • external parties source your information illegally • staff not following guidance in relation to the asset
Information availability and use	• failure to disclose critical information for case management/protection • failure to utilise the value of the information asset • failure to allow information to get to the right people at the right times	• staff not following guidance in relation to the asset • ICT failure (availability)

Risk category	Example of risk	Example of threat
Technology & cyber (IT systems)	• denial of service due to systems failure • corruption of data leading to delay in services	• denial of service due to an attack • spear phishing • espionage or crime campaign • data leaves the service in an uncontrolled manner
Process disruption	• established processes disrupted by new regulation or government guidance • focus on compliance with security processes and procedures at the expense of business performance	

Stand back and look at the threats to your assets and your response to them in the round. Have you over or under-protected anything? This is one of perspective and assessing whether you have got the balance right, taking into account all the potential risks and exposure, but not spending disproportionate amounts where it isn't necessary to do so.

Information risks are threats to:

- CONFIDENTIALITY – resulting in unauthorised access or disclosure
- INTEGRITY – resulting in inaccurate, incomplete or corrupted data
- AVAILABILITY – resulting in authorised users being unable to access information when required

6.2. Risk management

The best way to manage risks is to be aware of them and plan. Once you have identified your information asset consider the following:

- what organisational objectives and processes does it support?
- what is the asset there for? What would happen if you couldn't use the system or access the information on it?
- what are the outputs and outcomes that would be affected if there was a problem?
- by answering the questions above, you can then think of the next level of questions:
  - who has access to the assets?
  - understand what happens to the asset at each stage in its lifecycle
- manage the risk (refer to your organisations policy and guidance)
- follow best practice in information and records management

6.3. Risk acceptance / risk tolerance

The minimum measures organisations put in place for data handling and information security are designed to protect information. However it may not always be possible for organisations to work within these requirements.

Organisations will have processes in place for considering variations/exemptions to the prescribed minimum standards for protecting information. Any variations/exemptions exposes organisations to risks and are therefore only considered in exceptional circumstances and require sign off by your organisations SIRO.

Please refer to our intranet site for specific policy/guidance on risk acceptance/risk tolerance.
http://ros-intranet/policiesandprocedures/sia/information_risk_policy.pdf

7. Data sharing and privacy

7.1. What is personal information?

Personal information is any information or data that links a living identifiable individual or individuals (data subject) with information about them whose release would be potentially or actually detrimental to them, for example by:

- exposing them to identity theft or fraud, or
- breaching an expectation of privacy, reveal aspects of their personal life, e.g. financial circumstances, health records, court records, ethnic origin, religious beliefs, witness protection, protected occupations (e.g. intelligence, undercover operatives) etc., or
- putting them at risk of significant emotional stress, financial damage or actual physical harm

This must include as a minimum all data falling into one or both categories below. personal information should be classified as directed by your organisation under the government security classification (GSC) scheme.

A. Any information that links one or more identifiable living person with information about them whose release would put them at significant risk of harm or distress.

1. One or more of the pieces of information which can be used along with public domain information to identify an individual.	combined with	2. Information about that individual whose release is likely to cause harm or distress.
• name • addresses (home or business or both) • postcode • email • telephone number • driving licence number (driving licence number is included in this list because it directly yields date of birth and first part of surname) • date of birth		• DNA or finger prints • bank, financial or credit card details • mother's maiden name • national insurance number • tax, benefit or pension records • health records • employment record • school attendance or records • material relating to social services including child protection and housing

Sensitive personal data as defined by section 2 of the Data Protection Act (1998), includes racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health, sexual life, commission or any alleged commission of any offence, any proceedings relating to an offence committed or alleged to have been committed by the data subject.

7.2. Government security classification (GSC) scheme

The GSC sets out:

- the correct level of protection a document should be given
- procedures to be followed for the creation, distribution and destruction of a document
- the impact of the loss of or inappropriate access to a document

The table below lists the classifications in order of sensitivity, with TOP SECRET being used for the most highly sensitive information, and the type of security clearance required to access information.at the three levels:

TOP SECRET	Developed vetting (DV)	Allows regular and uncontrolled access to information and assets up to and including TOP SECRET
SECRET	Security check (SC)	Allows access to information and assets up to and including SECRET, with occasional and supervised access to TOP SECRET
OFFICIAL	Baseline personnel security standard (BPSS) and in particular circumstances Counter terrorist checks (CTC) may be required, for example a specific building	Allows access to information and assets within OFFICIAL with occasional and supervised access to SECRET

Please refer to our intranet site for specific policy/guidance on GSC.

7.3. Personal data users

A personal data user is any member of staff or contractor who has access to, or is involved in handling individual records containing personal data.

Although staff have a personal responsibility when handling personal data, as an IAO you are responsible for the activities of any personal data users who have access to the information asset you own. For example, ensure only those with a business need have access to the data.

7.4. Data sharing & transfer

The SPF states that, where information is shared for business purposes, organisations must ensure the receiving party understands the obligations and protects the assets properly. Before sharing data with a third party, ensure the following conditions are met:

- you have a legitimate business purpose to share the data, and you have the authority to do so
- you only share the bare minimum of data required
- the recipient has the need to know and the appropriate security arrangements for handling the data according to its classification are in place
- the mechanism used to transfer the data meets the minimum security standards stipulated by the classification
- conditions of use are set before the data is shared

A privacy impact assessment (PIA) and risk assessment must be conducted before data sharing is established.

7.5. Data sharing agreements

When information is shared with a third party there may be an associated security risk to the information. This may be caused, for example, by its potential proliferation and/or loss of immediate control. The SPF has put in place security requirements for the control of the information and management of the risks. Among these requirements are:

- information should be recorded as assets of the organisation
- each asset should have an IAO responsible for the guardianship, management and use of the asset, and
- when transferring data belonging to an asset, a data sharing agreement or memorandum of understanding should be agreed between the parties

IAOs should note that:

- the responsibility for drawing up a data sharing agreement or memorandum of understanding is that of the IAO responsible for the asset concerned. They should identify any additional risks presented by the proposed transfer recording these risks and drawing up the agreement to allow the risks to be managed
- all data sharing agreements must have the appropriate level of sign off, for example the SIRO or board

7.6. Encryption

RoS should:

- ensure that all portable devices and removable media used for mobile or remote working (e.g. laptops, PDAs, mobile phones, smart phones, memory sticks, external drives, DVDs/CDs etc.) are appropriately secured. Where possible, only approved mobile devices should be used. CESG should be consulted for advice and guidance where this is not possible, and

- manage risks proportionately through application of an appropriate mix of technical, procedural, personnel and physical controls and assign an appropriate level of protection to mitigate, and / or recover from, the potential loss or failure of those assets

The two statements above, although they do not specifically mention data sharing, describe steps which must be taken to secure our organisation's information, wherever it may be and during transit. The primary way in which this is achieved for digital information is through encryption, and this should be considered for all personal, or otherwise, sensitive data if it leaves our secure systems. RoS has a specific encryption product available to anyone who needs it, please contact the RoS security and information assurance (SIA) team (x3333) for more information.

7.7. Privacy impact assessments

What is a privacy impact assessment (PIA) and who is required to complete one and when?

A PIA is a risk management process which helps assess privacy risks to individuals in the collection, use and disclosure of information.

- identify privacy risks to individuals
- identify privacy liabilities to the organisation
- protect the organisations reputation
- help instil public trust and confidence

RoS require that PIAs are carried out when establishing a new process for transferring personal data to a third party; and for policy work when the approach envisaged will involve sensitive information on individuals.

As an IAO you will contribute to PIAs when the information relates to your asset . You should ensure you understand what this process involves and who else in your organisation may also need to contribute such as though with data protection responsibilities.

Please refer to our intranet site for specific guidance on PIAs http://ros-intranet/sections/finance-legal/legalservices/information-governance/privacy-impact-assessments.html.

Further information on PIA's can be found on the information commissioner's office website – see related links page at the end of this handbook.

8. Reporting requirements

8.1. Risk assessment and reporting

Information assets have risks associated with them such as the risk of losing the assets, having them fall into the wrong hands, getting corrupted or any number of other issues. Potential risks to each of the information assets you own should be identified and assessed. Those risks you consider outside the RoS risk appetite should be mitigated against and action plans developed. You may need to escalate these risks to appear on organisational or corporate risk registers.

8.2. Annual judgement for governance statement

The annual statement of assurance confirms that internal controls are being managed within RoS and that issues identified are being addressed.

IAOs have a responsibility to understand what information is held, in what form, how it is added and removed, who has access and why. They are required to understand, identify and control risks to the business in relation to their asset(s) and provide assurance to their SIRO annually.

9. Data loss incidents

A data loss could cause harm or distress to individuals. It could also have an impact on RoS reputation and inability to deliver business objectives.

A data loss could result in a breach of legislation (for example the DPA for personal information). Data losses reported to the information commissioner's office (ICO) could also result in a monetary fine for RoS.

Managing data loss incidents and breaches

On discovery of a breach, or a suspected breach it must be reported immediately to the SIA Team (x3333) who will escalate .

The SIA team usually maintain oversight of the response to all notified incidents when data has been lost or compromised and/or a breach to data handling procedures has occurred. This ensures that the incident is appropriately reported (for instance to the SIRO or ICO); risk assessed with lessons learnt reports produced, and that this occurs in an accurate and timely way.

10. Information assurance culture/behaviours

IAOs are not only responsible for identifying, understanding, managing, reporting and recording risks in relation to their Information assets, they also have a role in leading and fostering a culture that values, protects and uses information for the benefit of the public and their organisation.

IAOs need to champion good information handling and support information assurance culture change activities in their organisations.

IAOs have a particular responsibility to ensure they maintain an awareness of any policies or guidance in relation to information management (IM) and also ensure these are followed by those who have access to their information assets, which may include third parties.

IAOs have a responsibility to assist in the delivery of the RoS IA strategy.

RoS provide training to all staff in relation to information assurance/management and as an IAO you should encourage staff to undertake this training.

The RoS IA strategy provides more detail on our expect culture and behaviours

11. Information assurance governance and other key information management roles

As outlined in the introduction, the Cabinet Office mandated three key roles which all organisations must implement: accountable officer, senior information risk owner and information asset owner. There are other information assurance and information management roles in organisations.

Please see the table below which highlights the roles in RoS that may assist you in your role as IAO.

Accountable officer (AO)	has overall responsibility for having controls in place and ensuring information risks are managed. This is taken on by the role of the SIRO in RoS.
Senior information risk owner (SIRO)	leads the organisation's response on information risk. The SIRO in RoS may be required to submit an annual report providing an assessment of our information risks to our parent department.
Departmental security officer (DSO)	leads the organisation's response to security related matters. The DSO has overall responsibility for day to day protective security issues, ensuring that appropriate levels of security are in place in order to protect assets and contribute to overall national security.
Area information manager (AIM)	supports the IAO in promoting a strong security culture, ensuring new staff are given appropriate IA training, encouraging all staff to complete annual IA training, ensuring staff follow IA policies such as clear desk and screen policy, collate quarterly information asset register return and pass to IAO for sign off.
IT security manager	responsible for monitoring and assessing that RoS ICT infrastructure is maintained securely
Security and information assurance team	responsible for monitoring and assessing that RoS information assets are maintained securely
Data protection compliance officer	provides advice on data protection / privacy and authorises PIAs

12. Related links

Please find below some useful links that you may find helpful in your role as IAO.

Please refer to your organisations intranet site for further links that may be relevant to your organisation.

Information commissioner's office (ICO)

The UK's independent authority – set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

http://www.ico.org.uk

Scottish information commissioner

www.itspublicknowledge.info/home/ScottishInformationCommissioner.aspx

Cabinet Office

For the security policy framework (SPF)

https://www.gov.uk/government/publications/security-policy-framework

For the government security classification (GSC) scheme

https://www.gov.uk/government/publications/government-security-classifications

The National Archives

Lead organisation for delivering training and engagement programme for SIROs and IAOs

http://nationalarchives.gov.uk/services/publications/information-risk.pdf

http://www.nationalarchives.gov.uk/information-management/training/information-assurance-training.htm