Introduction to Risk Management for SIROs and IAOs

Workbook

Feb 2022

Name:

Job role:

Department:

Contents

Information Risk Management for SIROs and IAOs

Description

This learning contains practitioner level material aimed at all staff members who are involved in the management of information assets particularly SIROs and IAOs.

In this session you will learn why information risk is important and understand your responsibilities towards information assets.

An assessment is included at the end which you should use to test your understanding of the learning. You should check with your IG lead whether your responses need to be recorded and logged.

Author: Adapted by Digital Health and Care Scotland from NHS Digital sources.

Duration: Approx. 40 minutes

Learning objectives

By the end of this workbook you will understand:

- The need for information risk management within health and care.
- The recommended approach to information risk management.
- The role and responsibilities of the Senior Information Risk Owner (SIRO) and Information Asset Owners (IAOs) in providing assurance that information risk is being managed effectively.
- The role of Information Asset Administrators (IAAs) e.g. operational staff, to assist IAOs within larger organisations.
- What is meant by an organisation's information assets and how risks to them should be identified and managed.
- The key to successful information risk management.

Introduction

Information is a valuable resource. Its loss can damage reputations and services, its misuse can damage organisations and individuals.

Managing the risks to our information is clearly something we need to do, and be seen to do, well.

The ‘Review of Data Security, Consent and Opt-Outs’ (England, 2016) set out leadership obligations and data security standards that are applicable to all health and care organisations in England. In Scotland, we recognise the applicability of some of these recommendations, however there are fundamental differences in areas of opt-outs, for instance.

An area of the Review where Scotland agrees with our counterparts in England, is the expectation that CEOs and Executive Boards of health and care organisations must put effective information risk management high on their list of priorities.

You can find the ‘Review of Data Security, Consent and Opt-Outs’ (England, 2016) here: https://www.gov.uk/government/organisations/national-data-guardian/about.

The Scottish Government views and response to the Review in England, are reflected here: Chief Medical Officer, Public Health and Sport.dot (scot.nhs.uk)

The initial requirement for healthcare organisations to nominate a SIRO, assigning the role to executive level person, and putting the information risk high on the NHS Scotland agenda, was originally part of the NHSS Information Security Policy Framework 2015. Some elements of this policy, in particular those related to security controls in the framework, were amalgamated into the Scottish Public Sector Cyber Security Resilience Framework (Cyber resilience: framework and self assessment tool - gov.scot (www.gov.scot)).

In terms of leadership and responsibility over information risks, the new framework continues to re-inforce the requirement for SIROs, as a board-level individual who has overall accountability for the resilience of data and information systems (digital and non-digital); this is essential for the continuity of health and care services.

What is information risk?

A simple equation may help you understand the concept of risk more clearly. Risk is the outcome of a combination of threat and vulnerability.

Threat
+
Vulnerability
= Risk

Threat

Definition: A potential cause of an event (attack, accident or error) or source of danger. Threats are not always obvious, particularly to those who are not used to considering risks and how to avoid them.

An extended view of threats comes from the identification of missed opportunities arising for data and digital technologies to achieve the health and care strategic targets. Therefore, “threats” should not only be seen as sources of harm, but also as missed opportunities.

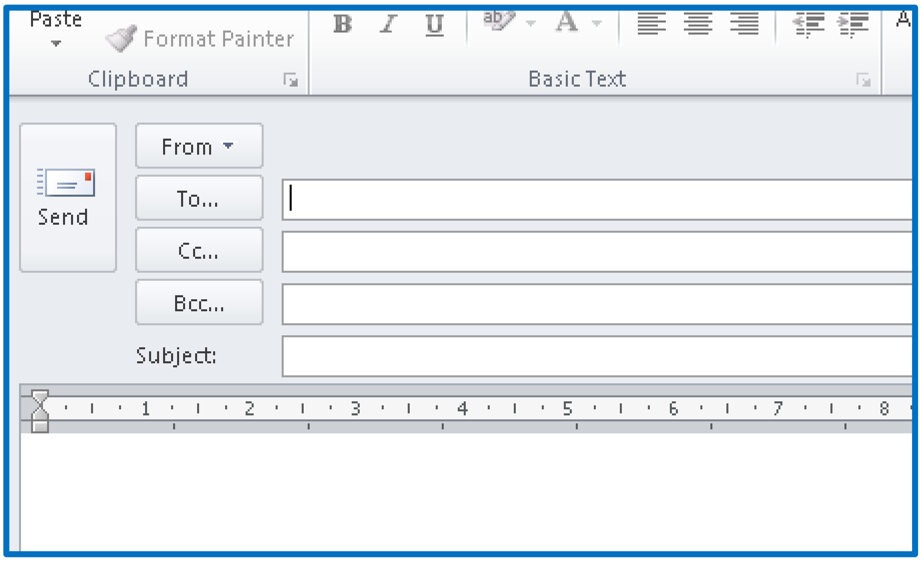
Vulnerability

Definition: A flaw or weakness of an information asset or group of assets that can be exploited by threat. This could be a design weakness in a system, an undocumented procedure or even an individual. You can help to reduce vulnerability by making yourself less open to attack – but you cannot avoid a threat completely unless you avoid the activity associated with the threat. As with threats, vulnerabilities are not always obvious and need to be identified and considered through appropriate risk management processes, training and education.

Scenario

Let us consider the well-publicised incident involving emailing patients.

A member of staff in the clinic sent a HIV related newsletter to the 781 subscribers of service.



In error the “to” field was used and not the blind carbon copy (“bcc”) field. The recipients of the e-mail could therefore see the e-mail addresses of all the other recipients.

What went wrong?

The ICO investigation report, which detailed the conclusions of the team that investigated this incident, found that there were a number of reasons why this happened. What do you think they might have been? Tick **<u>two or more options</u>** from the answers listed, and then check your answers with the feedback below.		
A	There was no specific training to remind staff to double check that the group e-mail addresses were entered into the correct field.	
B	The clinic did not inform the service users when they subscribed that their e-mail addresses would be used to send newsletters to them and to other service users by bulk mail.	
C	The Trust did not replace the e-mail account it was using with an account that could send a separate e-mail to each service user on the distribution list.	

Feedback:

All three options are true

There was no specific training to remind staff to double check that the group e-mail addresses were entered into the correct field - there was no training in place that covered how to treat mass emails.

The clinic did not inform the service users when they subscribed that their e-mail addresses would be used to send newsletters to them and to other service users by bulk mail - the organisation did not inform service users adequately how they were going to use their email addresses.

The Trust did not replace the e-mail account it was using with an account that could send a separate e-mail to each service user on the distribution list - they did not have a system in place to email service users separately or to enforce bcc for bulk mails.

What you'll do in this module

The incident at the Trust could have happened in any organisation that uses email to contact sensitive user groups or send information about sensitive topics. It demonstrates how essential it is to have the proper information risk management procedures and trained personnel.

The Government has a formal approach to managing information risk through a hierarchy of accountable roles.

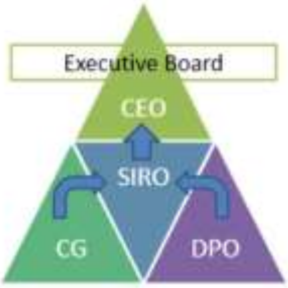
This workbook gives you the background information that will help you to undertake the role of the Senior Information Risk Owner (SIRO) or of an Information Asset Owner (IAO).

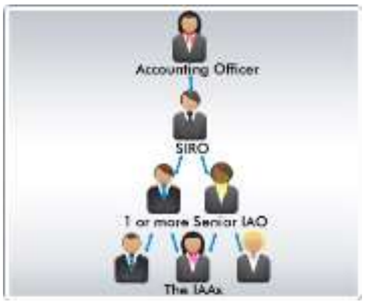
You'll recall that the learning objectives for this workbook are:

- The need for information risk management within health and care.
- The recommended approach to information risk management.
- The role of SIROs and IAOs in providing assurance that information risk is being managed effectively.
- The role of Information Asset Administrators (IAAs) e.g. operational staff, to assist IAOs within larger organisations.
- What is meant by an organisation's information assets and how risks to them should be identified and managed?
- The key to successful information risk management.

How should information risk be approached?

The **key requirement** is for information risk to be managed in a robust manner within work areas (and not be seen as something that is the sole responsibility of IT or IG staff) and for information assurance to be provided in a consistent manner.





IG Team
Data Custodians
Service Managers-Directors
ISO Information Security Officer
Records Management staff
SIRO Senior Information Risk Owner
IAO Information Asset Owner
IG Leads
DPO Data Protection Officer
Caldicott Guardian
TEAMWORK

To achieve this, a structured approach is needed, building upon the existing Information Governance Framework within which many parts of the health and care are already working. This structured approach rests upon the identification of an organisation's information assets and assigning 'ownership' of those assets to senior accountable staff.

What is information risk management?

Information risk is inherent in all administrative and business activities and everyone working for or on behalf of health or care organisations continuously manages information risk.

Why is information risk management so important?

The aim of information risk management is not to eliminate risk, but rather to provide the structural means to consistently identify, prioritise and manage the risks involved in all business activities. It requires a balance between the cost of managing and treating information risks, and the anticipated benefits that will be derived.

What are the objectives of information risk management?

The objectives are to:

- Ensure continuity of service, by protecting the organisation, its staff and its patients / service users from information risks where the likelihood of occurrence or the consequences matter.
- Meet legal or statutory requirements.
- Assist in safeguarding the organisation's information assets (digital and non-digital).

How can these objectives be achieved?

The way to achieve these objectives is to:

- Provide a consistent framework in which information risks will be identified, considered and addressed in key approval, review and control processes.

- Encourage proactive management of risk rather than reactive incident response.

Summary

You've reached the end of this introductory section. Here's a summary of the main points.

- Health and care organisations have responded to Government instructions and guidance that set out the responsibilities for information risk management, by developing a structured approach in which the information assets of an organisation are identified and ownership of them is assigned to senior accountable staff.
- The SIRO provides assurances to the Accounting Officer, CEO, Managing Director and the wider Executive Board.
- The aim of information risk management is not to eliminate all risk but to provide a framework in which risk can be reliably identified, prioritised and managed, so that health and care organisations are protected from potentially adverse consequences.
- Risk management should also aim for maximising the data and digital opportunities that good things may happen, and not only focus on the adverse impact. This can be seen as the risk of a missed data and digital opportunities to achieve organisational goals or strategies. Risk and Opportunity: How can risk be good? Video 11min

Information risk management structure

Introduction

In this topic you're going to look at the information risk management (IRM) structure in more detail.

IG Team
Data Custodians
Service Managers-Directors
ISO Information Security Officer
IAO Information Asset Owner
Records Management staff
SIRO Senior Information Risk Owner
IG Leads
DPO Data Protection Officer
Caldicott Guardian
TEAMWORK

The structure is based on tried and tested risk management techniques and is in line with the guidelines published by the Cabinet Office for the public sector.

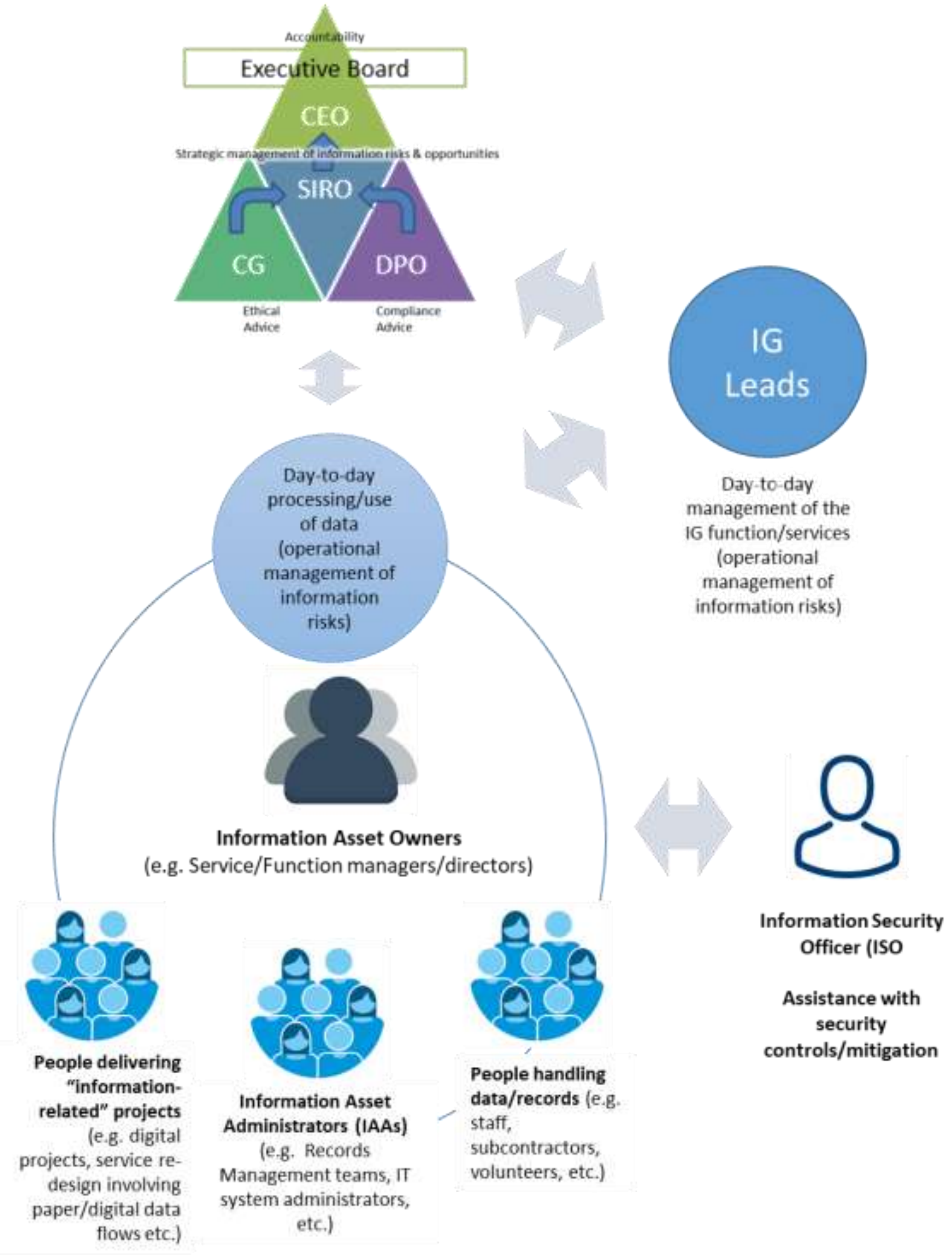
By the time you've completed this topic you should understand:

- The IRM structural model.
- The main responsibilities of the SIRO and IAO.
- The resources available to support staff in these roles.

The IRM structural model

Key roles in the IRM model

Here are some diagrams that illustrate the IRM structural model.



Day-to-day processing/use of data (operational management of information risks)

Day-to-day management of the IG function/services (operational management of information risks)

Information Asset Owners
(e.g. Service/Function managers/directors)

Information Security Officer (ISO

Assistance with security controls/mitigation

People delivering "information-related" projects (e.g. digital projects, service re-design involving paper/digital data flows etc.)

Information Asset Administrators (IAAs) (e.g. Records Management teams, IT system administrators, etc.)

People handling data/records (e.g. staff, subcontractors, volunteers, etc.)

Accounting Officer

The Accounting Officer (CEO/Managing Director or equivalent) has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. Information risks should be handled in a similar manner to other major risks such as financial, legal and reputational risks. Reference to the management of information risk and associated information governance practice is required in the Annual Governance Statement which the Accounting Officer is required to sign.

Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is an executive Board / senior management team member who is familiar with information risks and provides the focus for the management of information risk at that level. He/she must provide the Accounting Officer with assurance that information risk is being managed appropriately and effectively across the organisation and for any services contracted for by the organisation.

Information Asset Owner

IAOs are responsible for managing information risk associated to the Information Assets they are responsible for on behalf of the organisation, and providing assurances to the SIRO.

Information Asset Owners (IAOs) are senior individuals involved in running the relevant business. 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 assets they ‘own’ and to provide assurance to the SIRO on the security and use of the assets. In larger organisations, an IAO might be a department head, for example.

Data Protection Officer (DPO)

DPOs are required, by UK GDPR legislations, to provide advice on areas of data protection compliance and risks to the rights and freedoms of people. This advice include all areas of the data protection principles, which include fairness, proportionality and security, amongst others.

Caldicott Guardian (CG)

Caldicott Guardians provide advice on areas of fairness and ethical use of patient’s data and Duty of Confidentiality.

Information Security Officer (ISO)

ISOs provide advice and assist IAOs, Caldicott Guardians and Data Protection Officers with specific security controls that should or can be implemented to protect the information assets and the rights and freedoms of people, in particular, their privacy rights.

Data Custodian

Data Custodians assist IAOs looking after the information assets they are responsible for. Sometimes, Data Custodian functions are embedded in other roles, e.g. Database Managers, Data Servers Managers, Information Systems Managers etc.

Information Governance (IG) Leads

Information Governance Leads manage teams that assist SIROs and IAOs in the setting of information security and data protection policies, procedures, processes and tools to assist the IG tasks, supporting the organisation with the implementation of such policies, monitor adherence and improve IG processes.

Information Asset Administrator

Information Asset Administrators (IAAs) ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date. These are optional roles, not all organisations will have IAAs, but in a larger organisation this role could be filled, for example, by an operational member of staff who is responsible for one or more information assets.

Records Management staff

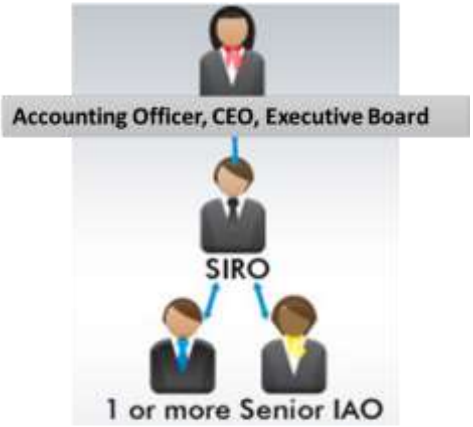
Health and corporate records are valuable Information Assets. HRMs are responsible for the overall development and maintenance of health and corporate records management practices throughout the organisation. They have responsibility for drafting guidance to support good records management practice in relation to health records and for promoting compliance with the Records Management Code of Practice, in such a way as to ensure the efficient, safe, appropriate and timely retention and retrieval of patient information.

Archivists also play a key role in the preservation of valuable information assets. They are responsible for collecting, cataloguing, preserving and managing appropriate access to valuable historical information. Archivists liaise with records managers, data protection officers and other information governance professionals to train and identify relevant material of historical value ensuring transfer to archival preservation. Note that valuable historical information may be ‘born digital’ and exist as electronic files as well as traditional paper archives.

At the discretion of each organisation, some of these roles may also have delegated powers from the SIRO or the IAOs to approve certain types of requests for processing data or access digital systems (e.g. pre-approved, well-known scenarios, and low risk requests). It is important to remember that delegation does not transfer accountability, which remains with the designated IAO and, ultimately, with the SIRO.

Why this model for managing information risk?

The aim is to ensure that information risk management is seen as a key responsibility for appropriate staff and that they are accountable for outcomes.



You need to ensure that information risk management:

- is comprehensive (this means you need to make sure it covers **all** the information assets in the organisation);
- takes full advantage of existing authority and responsibility structures (i.e. don't reinvent something if it is already there);
- associates tasks with appropriate management levels;
- avoids unnecessary impacts on day to day business;
- ensures that all the necessary activities are discharged in an efficient, effective, accountable and visible manner.

We will next look more closely at the responsibilities of the SIRO and the IAOs.

The SIRO’s role and responsibilities

The role and responsibilities of the SIRO fall into four main categories.

Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers

The SIRO needs to find ways of actively fostering such a culture, both across the organisation and with its business partners. For information risk management to be effective, it’s essential that everyone in the organisation is aware of its importance and receives appropriate training. Sometimes people are nervous about risk and about reporting it. If risk is reported, beneficial changes can be made to mitigate it.

Owning the organisation’s information risk and incident management framework

To ensure that the information risk and incidents are managed properly, the SIRO needs to be familiar with the organisation’s business and goals, particularly in relation to the way it uses internal and external information assets.

IAOs need to be identified for all the organisation’s information assets. The SIRO needs to make sure the IAOs understand their roles and have appropriate support.

The aim is to mitigate risk, not eradicate it. This means that there may be times when there is an information ‘incident’. The SIRO needs to have response and management procedures in place for when such an incident occurs. This includes the reporting of ‘perceived’ or ‘actual’ Serious Incidents Requiring Investigation (SIRIs) involving data loss or confidentiality breach but is of course far wider. The SIRO also needs to establish a corporate culture in which, when things do go wrong, people are confident enough to share the lessons learned.

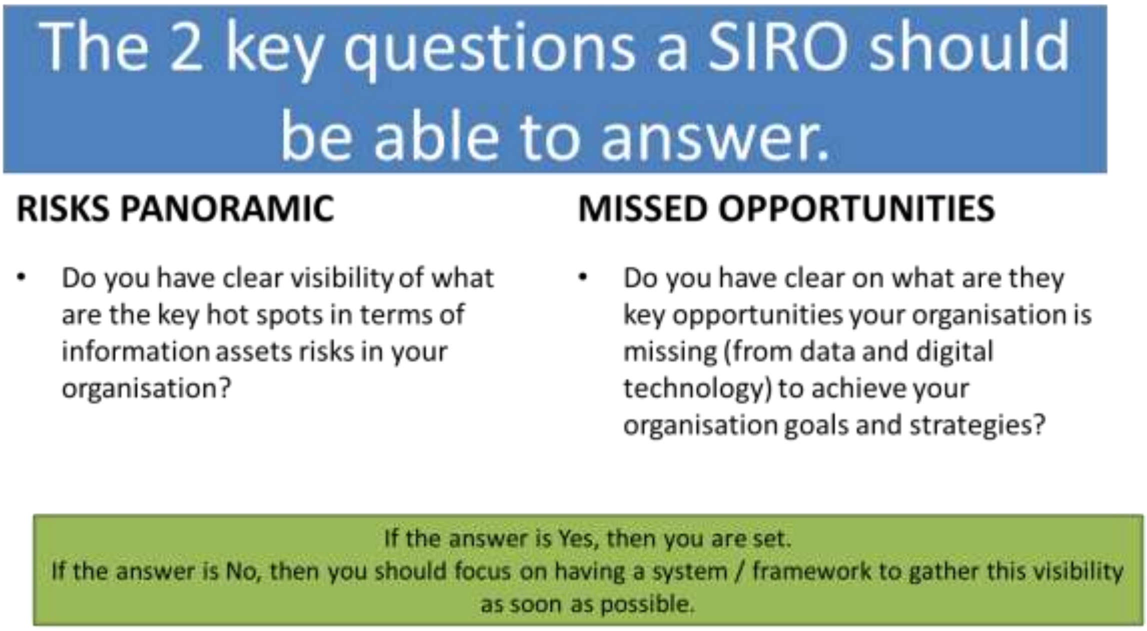
Owning the organisation’s overall information risk policy and risk assessment processes and ensuring they are implemented consistently by IAOs

This is a very broad ranging responsibility, but amongst other tasks the SIRO has to do the following:

- Act as an IRM focal point dealing with risk resolution across the organisation and with other escalated risk issues raised by IAOs, Information Security Officers, Auditors or others.
- Initiate and oversee a comprehensive programme of work that identifies, prioritises and addresses IG risk and systems’ accreditation for all parts of the organisation, with particular regard to information systems that process personal data.
- Ensure that privacy impact assessments are carried out on all new projects when required, in accordance with the guidance provided by the Information Commissioner (and later under the General Data Protection Regulation), and that information risk assessments are completed on a quarterly basis, taking account of all available Information Governance and data security guidance from Digital Health and Care (Scottish Government) and the (NIS) Health Competent Authority, and other competent bodies.
- Develop and implement an information risk policy that is appropriate to all departments of the organisation and their uses of information, setting out how compliance will be monitored.
- Ensure that information risk management methods and standards are documented, applied and maintained consistently throughout the organisation’s information risk assessment process and management framework.
- Review all key information risks faced by the organisation and its partners, on a regular basis, ensuring that mitigation plans are robust. These risk assessments and mitigation actions will need to benefit from appropriate independent scrutiny so that the identified risks can inform investment decisions including outsourcing.

Advising the Chief Executive, Executive Board and relevant Accounting Officer on the information risk aspects of his/her Annual Governance Statement

Building on the quarterly reviews of information risk that need to be conducted by the IAOs and the annual assessment of IG performance conducted through the centrally provided tool, the SIRO has to sign off an annual assessment of organisational compliance.



The 2 key questions a SIRO should be able to answer.

RISKS PANORAMIC

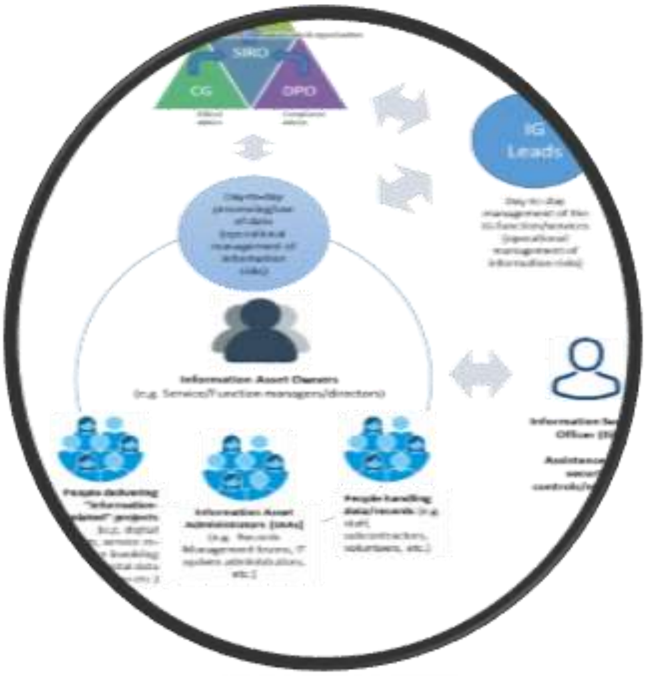
- Do you have clear visibility of what are the key hot spots in terms of information assets risks in your organisation?

MISSED OPPORTUNITIES

- Do you have clear on what are they key opportunities your organisation is missing (from data and digital technology) to achieve your organisation goals and strategies?

If the answer is Yes, then you are set.
If the answer is No, then you should focus on having a system / framework to gather this visibility as soon as possible.

The role of IAOs


SIRO
CG
DPO
IG Leads
Information Asset Owners
(e.g. Service/Function managers/directors)
Information Asset Administrators (IAAs)
People handling data/records (e.g. staff, subcontractors, volunteers, etc.)

Who is the IAO?

The Information Asset Owner (IAO) will be a senior member of staff who is the nominated owner for one or more identified information assets of the organisation.

The IAO and compliance

It is a core IG objective that all Information Assets (IAs) of the organisation and those held jointly with other organisations are identified and that the business importance of those assets is established.

IAOs must work with IG Leads and DPOs to ensure they can evidence compliance with the UK GDPR Accountability principle for Information Assets they are responsible for, on behalf of the organisation.

Whilst building upon the existing guidance on the management of information assets, the new UK GDPR emphasis on accountability requires that existing arrangements are reviewed to ensure IAOs have the required seniority and authority.

IAO seniority

It is important to distinguish IAOs from more junior staff who have been assigned responsibility for day to day management of information assets, but are not directly accountable to the SIRO. The SIRO/IAO hierarchy identifies accountability and authority to effect change where required and to mitigate against identified risk.

IAOs working together

It’s also important that IAOs within an organisation work closely together to ensure there is comprehensive information asset ownership and clear understanding of individual responsibilities and accountabilities. This is particularly true when IAs are shared by different parts of the organisation.

The IAO’s responsibilities

The responsibilities of the IAO fall into four main categories.

1. Information security culture

Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers

To do this the IAOs need to:

- Understand the SIRO’s plans to achieve and monitor the right IG culture, across the organisation and with its business partners.
- Take visible steps to support and participate in that plan (including completing own training).
- Ensure that staff understand the importance of effective Information Governance and receive appropriate education and training.
- Consider whether better use of any information held is possible, within applicable Information Governance rules, or where information is no longer required.

2. Information as a valuable asset and data flows.

Knowing what information comprises or is associated with the “information asset”, and understands the nature and justification of information flows to and from the asset.

This requires the IAO to:

- Maintain an understanding of ‘owned’ assets and how they are used.
- Approve and minimise information transfers while achieving business purposes.
- Approve arrangements where it is necessary for information to be put onto portable or removable media like laptops and USB drives and ensure information is effectively protected.
- Approve the disposal mechanisms for information from the asset.

3. Access to the information asset is understood and monitored.

Knowing who has access to the asset, whether system or information, and why, and ensures access is monitored and compliant with policy

The IAO needs to ensure that:

- He/she understands the organisation’s policies on the use of information and the management of information risk.
- Decisions on access to IAs are taken in accordance with IG good practice and the policies of the organisation.
- Access provided to an asset is the minimum necessary to satisfy business objectives.
- The use of the asset is checked regularly and that use remains in line with policy.

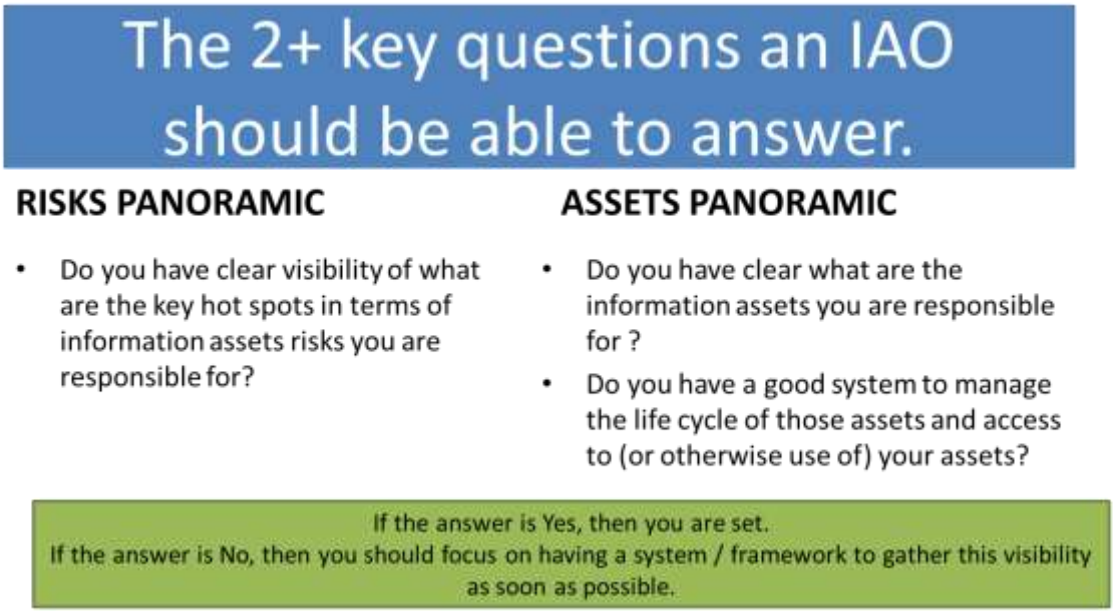
4. Management of the information risk for the asset.

Understanding and addressing risks to the asset, and providing assurance to the SIRO.

The IAO needs to:

- Seek advice from IG subject matter experts, including DPOs, Caldicott Guardians, Information Security Officers, etc. when reviewing information risk.

- Conduct information security and privacy impact assessments for all new proposals to use, change, access or decommission the information assets “owned” by the IAO.
- Undertake regular information risk assessment reviews (quarterly) for all ‘owned’ information assets and report to the SIRO, ensuring that information risks are identified, documented and addressed.
- Escalate risks to the SIRO where appropriate and to make the case where necessary for new investment to secure ‘owned’ assets.
- Provide an annual written assessment to the SIRO for all assets ‘owned’ by them.



The 2+ key questions an IAO should be able to answer.

RISKS PANORAMIC

- Do you have clear visibility of what are the key hot spots in terms of information assets risks you are responsible for?

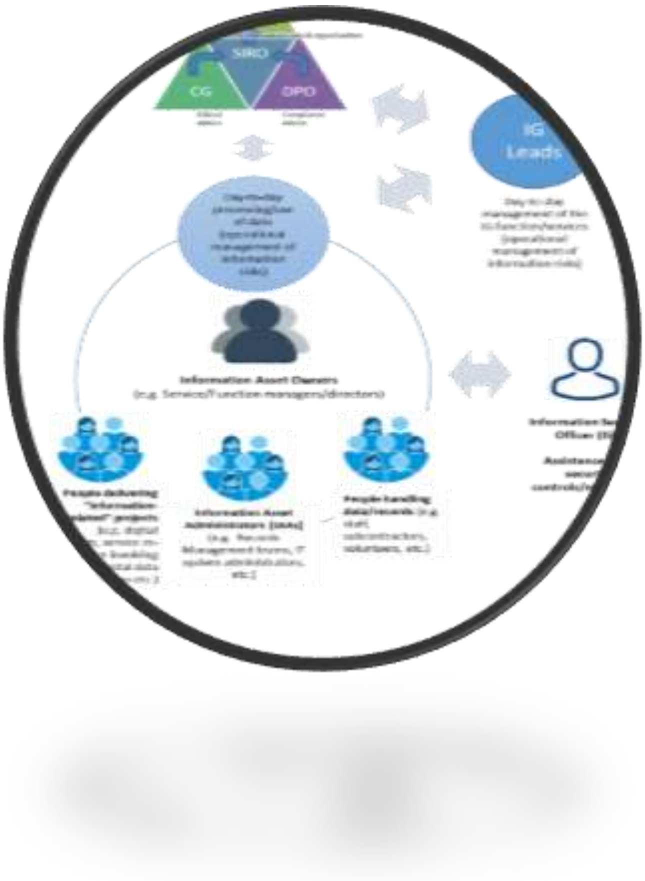
ASSETS PANORAMIC

- Do you have clear what are the information assets you are responsible for ?
- Do you have a good system to manage the life cycle of those assets and access to (or otherwise use of) your assets?

If the answer is Yes, then you are set.
If the answer is No, then you should focus on having a system / framework to gather this visibility as soon as possible.

Support for SIROs and IAOs

It's important to realise that these key roles don't work in isolation. They need to fit into the wider organisational structure, i.e. everybody needs to be aware of Information Governance and play their part. SIROs and IAOs need to know who they will receive support from.


SIRO
CG
DPO
IG Leads
Information Asset Owners
(e.g. Service/Function managers/directors)
Information Asset Administrators (IAAs)

Accountability

Information Risk Management is a component of Information Governance but the introduction of an accountable hierarchy that sits with business managers rather than specialist staff requires a new approach.

The SIROs and IAOs need support to carry out their roles effectively.

Who can provide support ?

Among those who can support IAOs and SIROs to identify and mitigate against information risk are Caldicott Guardians, information security experts, data protection staff, and information governance generalists.

What support can be provided ?

The support they can provide includes staff training and support, advising on IAO information risk reviews, assisting with the delivery of mitigating actions and ensuring that the organisation's approach to managing information risk is accurately reflected in the Annual Governance Statement.

Other resources

Whilst there will be many lessons learned from this approach to information risk management, there are already a range of materials provided to support health and care organisations.

The Information Governance and Assurance Unit (Digital Health and Care Directorate, Scottish Government)

The Information Governance and Assurance Unit (Digital Health and Care Directorate, Scottish Government) is the authoritative source of advice and guidance about the rules on using and sharing information in health and care in Scotland.

The National IG Programme, as part of the Digital Health and Care Strategy and the Health and Care Data Strategy within the Scottish Government, envisage the creation of a national body that will become the authoritative source of advice and guidance, and will be formed by experts and representatives of key stakeholders across health and care in Scotland.

The Information Governance and Assurance Unit offers advice and support, develops networks, publishes guidance, endorses guidance produced by others, and works with local and national organisations, including National Services Scotland, Public Health Scotland, COSLA, NHS Education for Scotland, etc. to improve knowledge and practice of information governance across the health and care system.

You can access guidance, publications and other resources from their website at: https://www.informationgovernance.scot.nhs.uk/

The Information Governance and Assurance Unit can be contacted via:

DHCIG@gov.scot

(NIS) Health Competent Authority (Scotland)

Scottish Ministers are considered to be the Competent Authority (CA) for Health in Scotland. They have devolved operational duties to the Scottish Government's Digital Health and Care Division.

The functions of the CA are to:

- Provide support, training and guidance on compliance requirements.
- Deliver regulatory responsibility for compliance monitoring, oversight and enforcement of the NIS Regulations.
- Issue penalties for non-compliance.

The CA has produced a range of support material to aid compliance with the NIS Regulations, such as guidance publications and template reporting forms. The documents are developed on an ongoing basis. We welcome feedback and comments to inform future versions.

The CA can be contacted by email at HealthCA@gov.scot

The National Cyber Security Centre (NCSC)

The NCSC are the UK's independent authority on cyber security. Further information regarding NIS can be located on their site:

- https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

IG and Security Networks

Across health and care in Scotland there are a number of networks, enabling information governance practitioners to meet and share ideas and materials. Examples are:

- The National Caldicott Guardians Forum (Scotland)
- The NHS IG Leads Forum
- The NHS Information Security Forum
- The Public Sector Data Protection Officers Network

The aim of the networks is to help reduce isolation at a local level by supporting peer engagement. The networks give you the chance to speak to people who can assist with the information governance agenda and engage on key issues.

At the moment there is not an specific network for SIROs or IAOs, however, there is a workstream within the National IG Programme to consider the best approach to establish a suitable network for this group.

The National IAO

The Digital Health and Care Director is the IAO for National Information Assets funded and commissioned centrally by Scottish Government, on a "Once-for-Scotland" approach.

The National IAO may delegate the operational responsibility over specific Information Assets to organisations such as National Services Scotland, Public Health Scotland or NES (Digital services), for instance.

The accountability over National assets is not transferred.

The National Caldicott Guardian

Scotland does not have a National Caldicott Guardian, however, the Chief Medical Officer (Scottish Government) has the responsibility to provide advice on the ethical use of patient's data, including Duty of Confidentiality matters and the necessity and proportionality of using data assets or digital technologies for direct patient care, as well as for secondary purposes. These already existing responsibilities will be reflected in the Scottish Caldicott Guardian for Health and Care, as part of the National IG Programme 2022/2024.

All NHS Scoltand health boards, including those with a National remit, have substantive Caldicott Guardians that can be approached using their contact details available on NHS Inform: https://www.nhsinform.scot/care-support-and-rights/health-rights/confidentiality-and-data-protection/how-the-nhs-handles-your-personal-health-information#caldicott

Public Benefit and Privacy Panel for Health and Social Care (NHSS HSC-PBPP)

The HSC-PBPP is a governance structure of NHSScotland (NHSS). It was established with delegated authority from NHSS Chief Executive Officers and the Registrar General of National Records of Scotland (NRS), for the NHS Central Register (NHSCR). Its remit is to carry out information governance (IG) scrutiny of requests for access to health data for purposes of health and social care administration, research and other well-defined and bona fide purposes, on behalf of individual data controllers.

The HSC-PBPP acts as the final arbiter of requests which fall within its remit, but does not replace any existing or future requirements for ethical review or approval. In this sense, SIROs and IAOs need to understand their accountabilities are not delegated, but PBPP can scrutinise on their behalf a recommend corrective actions for proposals to access NHS data or information systems.

The HSC-PBPP has 'dotted line' reporting to Scottish Government Digital Health and Care Directorate (formerly "eHealth").

The HSC-PBPP has a formal mandate to scrutinise requests to use NHSS-controlled data, and the NHSCR, controlled by the Registrar General, for research, healthcare planning, audit, or other well-defined and bona fide purposes. Its principal focus is on what are deemed national data-sets, data from more than one NHS Board, or cases involving data from one NHS Board which are highly complex, contentious or have national implications.

Summary

You've reached the end of this topic. Here's a summary of the main points.

What is the information risk management (IRM) structure?

The model consists of four layers: at the top is the Accounting Officer, to whom the Senior Information Risk Owner provides assurances. The Information Asset Owners IAOs are responsible for ensuring that information risk is managed appropriately and for providing assurances to the Senior Information Risk Owner (SIRO). In some organisations, Information Asset Administrators (IAAs) support the IAOs by managing information assets on a day to day basis.

SIROs and IAOs may seek advice from Caldicott Guardians and Information Security Officers. Consultation with Data Protection Officers is mandated in UK GDPR law.

IG leads may offer support to SIROs and IAOs. The support arrangements may vary across health boards.

What are the main responsibilities of the people involved in IRM?

The Accounting Officer (CEO / Managing Director or equivalent) has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level.

The SIRO is an executive Board / senior management team member who is familiar with information risks and provides the focus for the management of information risk at board level. The SIRO is responsible for:

- leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers;
- owning the organisation's information risk and incident management framework;

- owning the organisation’s overall information risk policy and risk assessment processes and ensuring they are implemented consistently by IAOs;
- advising the chief executive or relevant accounting officer on the information risk aspects of his/her statement on internal controls.

IAOs are responsible for:

- leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers;
- knowing what information comprises or is associated with the asset, and understands the nature and justification of information flows to and from the asset;
- knowing who has access to the asset, whether system or information, and why, and ensures access is monitored and compliant with policy;
- Understanding and addressing risks to the asset, and providing assurance to the SIRO.

Other people, including, Data Protection Officers, Caldicott Guardians, information security experts, and information governance generalists, support IAOs and SIROs to identify and mitigate against information risk.

What are the main characteristics of the approach to IRM?

The approach needs to:

- be comprehensive - this means you need to make sure it covers all the information assets in the organisation;
- take full advantage of existing authority and responsibility structures - i.e. don't reinvent something if it is already there;
- associate tasks with appropriate management levels;
- avoid unnecessary impacts on day to day business;
- ensure that all the necessary activities are discharged in an efficient, effective, accountable and visible manner.

What is an information asset?

In this topic you're going to look at identifying information assets (IAs) and consider how information risk management should be conducted. The comprehensive identification of IAs is essential for effective management of information risk.

Which of these items do you think are IAs? Tick **two or more options** from the answers listed below, then read the feedback to check your answer.		
A	Audit data	
B	Laptop	
C	Data encryption utilities	
D	The server room air conditioning, which is part of the information system	
E	System administrator's skills and experience	
F	Business continuity and disaster recovery plans for a care records system	

Feedback: They're all examples of IAs.

IAs are identifiable and definable assets owned or contracted by an organisation which are 'valuable' to the business of that organisation. They come in many shapes and forms, as the list shows you. You'll find out more about this on the next screen.

Information Assets may also be referred to as digital assets, but not on IA are digital e.g. paper records.

Also, in the rest of the topic you'll see how important it is to take all your IAs into account when managing information risk.

Examples of information assets

As IAs vary so considerably from organisation to organisation, it’s impossible to give a comprehensive list. Which of these items do you think are IAs?

2
3
5
Contract
4
6
1

Tick **two or more options** from the answers listed below, then read the feedback to check your answer.			
1	Personal information content (A paper file with an ID photo attached)	• Databases and data files. • Backup and archive data. • Audit data. • Paper records and reports. • Case notes.	
2	Software (Laptop showing spreadsheet)	• Applications and system software. • Data encryption utilities. • Development and maintenance tools.	
3	Other information content (Laptop showing database)	• Databases and data files. • Backup and archive data. • Audit data. • Paper records and reports.	
4	Hardware (Smart Phone)	• Computing hardware including PCs, laptops, tablets, networks, printers, smart phones, communications devices e.g. iPhone / android smart phones and USB drives.	
5	System/process documentation (Document labelled ‘Contract’)	• System information and documentation. • Operations and support procedures. • Manuals and training materials. • Contracts and agreements. • Business continuity and disaster recovery plans.	
6	Miscellaneous (An individual)	• Environmental services, e.g. power and server room air conditioning. Servers are dependent on the air-conditioning system to operative effectively and optimally. • People skills and experience.	

Feedback: They’re all IAs

Categorising and managing information assets

As you've seen, IAs come in many shapes and forms. However, they all share a set of key characteristics.

What are the key characteristics of information assets?

All IAs:

- are identifiable and their ownership is assignable to an Information Asset Owner (IAO) within the organisation;
- have 'value' to the organisation and contribute to satisfying its business objectives;
- are not easily replaceable if lost or damaged beyond repair without significant new financial investment in time or resource;
- form part of the organisation's overall asset inventory such that their business importance is understood and their risks are managed.

How should information assets be categorised?

As you've seen IAs can be categorised by what they are – for example, personal information or hardware and software.

However, it makes good risk management sense to group all of the components that relate to the same information asset or business process together. For example, you might put an IT system, its system documentation, the data held within it and the skills of staff who administer it into one IA category.

NHS Scotland provides a range of optional tools to assist you with developing information asset registers and managing information assets.

How are information assets managed?

It is vital that all health and care organisations adhere to Government policy and establish programmes that ensure their IAs are identified and assigned to an IAO.

Many organisations will already have information asset registers as described in the centrally provided assessment tool (at the time of writing, the NHS Information Governance Toolkit). These should already capture details of the main information systems and record collections.

However, the focus on information risk management broadens the definition of IAs. Therefore, the SIRO should review the organisation's information asset register to ensure it is complete and robust.

Which information assets should be given priority?

You will be aware that the 'risk appetite' across the public sector, where personal data is the information asset in question, is currently extremely low. Therefore where information risk management programmes are constrained by time and resources you must give priority to information assets which comprise or contain personal information about patients or staff.

Managing information risks

At the start of this module we said that information risk is the product of threat and vulnerability. Let us look at the definitions of these in a little more detail with examples.

Information Risk Management
Threat
+
Vulnerability
= Risk

Threat: A potential cause of an event (attack, accident or error) or source of danger. Threats are not always obvious, particularly to those who are not used to considering risks and how to avoid them.

Vulnerability: A flaw or weakness of an information asset or group of assets that can be exploited by threat. This could be a design weakness in a system, an undocumented procedure or even an individual. You can help to reduce vulnerability by making yourself less open to attack – but you cannot avoid a threat completely unless you avoid the activity associated with the threat. As with threats, vulnerabilities are not always obvious and need to be identified and considered through appropriate risk management processes, training and education.

Risk: The probability of a vulnerability being exploited, potentially leading to a degree of loss of confidentiality, integrity, or availability of an information asset. For example, an opened email attachment that could contain malware and that may infect the system.

Acceptable risks

So, you know that Information Risk Management is about determining and managing an acceptable level of risk. But what is an 'acceptable level' of risk? Well, the truth is there's no standard right or wrong answer to that question. This will depend on various business factors.

The definition of acceptable risk, and the approach used to manage risk, may vary for every organisation. Every organisation manages risk, but not always in a way that is obvious, consistent or repeatable.

Implementing a well-defined information risk management structure and process helps to ensure that everyone within the organisation understands the risks they face and knows the practices to adopt to manage, control or eliminate them.

Although the phrase 'Information Risk Management' may sound off-putting, it should actually be viewed as a constructive, experience improving process and not a limiting one.

It is not a way of identifying reasons why a course of action should not be pursued. Rather it is a way of enabling a direction to be taken on a fully informed basis, being aware of the potential risks involved, and identifying controls or countermeasures to mitigate those risks to an acceptable level.

Successful information risk management

The benefits of Information Risk Management depend on how it is planned, structured and how widely it is embraced within your organisation. The less consideration and effort that goes into it, the fewer benefits it produces. So what's the key to successful Information Risk Management?

Embed it consistently within the structure of your organisation

The best information risk management processes are the ones that are firmly **embedded** into the overall management and working culture of your organisation.

Information risk management should not be a hollow 'box ticking' exercise, but synonymous with good management and good governance in general.

It should be seen as a two way process, which both feeds information **up** through the organisation to help strategic planning and underpin corporate assurance, but also **downwards** to help manage risks by supporting employees and providing the necessary guidance and resources.

The information risk management function

The information risk management function may feature within a range of different job roles. However, it is for those individuals with information risk management responsibility to ensure that information risk is assessed and considered on similar terms as other risks faced by the organisation, e.g. financial, legal and operational risks.

Such staff should be fully aware of the strategic business goals of their organisation, as well as understanding how a disruption to or failure of information assets they have responsibility for can impact on those goals. They will typically undertake risk management functions for one or more information assets and will work with other relevant staff to assess and address identified information risks. Depending on the size and complexity of the organisation, information risk management may be a dedicated role.

Don’t eliminate risk altogether

No risk management process can create a completely risk-free environment – nor should it aim to.

Eliminating organisational risk altogether would go against the best interests of any organisation. If we never took risks, we would never improve the way we work or realise any opportunities.

Instead, effective risk management helps to manage the risks associated with an opportunity so that it is more likely to be achieved. It helps to ensure that damaging things are less likely to happen.

This means that risk management can actually help your organisation to take on innovative and exciting activities that have a higher level of risk, because everyone understands the risks involved and how to keep them at an acceptable level. This is also true for information risks of the organisation.

Summary

You’ve reached the end of this topic. Here’s a summary of the main points.

What are information assets?

Information Assets (IA) are identifiable and definable assets owned or contracted by an organisation which are ‘valuable’ to the business of that organisation.

What form do information assets take?

IAs come in all shapes and forms but some of the component categories you will encounter include:

- personal and other information content
- software
- hardware
- system/process documentation
- environmental services
- people’s skills and experience

What is the Government policy about information assets?

It is vital that all health and care organisations establish programmes that ensure their IAs are identified and assigned to an IAO. The SIRO should oversee a review of the asset register to ensure it is complete and robust.

What is information risk management?

Information risk management is the process of determining an acceptable level of risk; assessing the current level of risk; taking steps to reduce risk to the acceptable level, and maintaining or improving that level of risk.

What is information risk?

Information risk is the probability of a vulnerability being exploited, potentially leading to a degree of loss of confidentiality, integrity, or availability of an information asset.

What is the key to successful information risk management?

- Firmly embed overall information risk management processes into the overall management and working culture of your organisation.
- Ensure individuals with information risk management responsibility assess and consider information risk on similar terms as other risks faced by the organisation.
- Don’t attempt to eliminate organisational risk altogether as to do so would go against the best interests of any organisation.

Module Summary

You’ve reached the end of this workbook ‘Introduction to Risk Management for SIROs and IAOs’.

You’ve seen that the aim of information risk management is not to eliminate risk, but rather to provide the structural means to reliably identify prioritise and manage the risks involved in all business activities.

Senior Information Risk Owners and Information Asset Owners play a crucial role in this process.

You should understand:

- The need for information risk management within health and care.
- The recommended approach to information risk management.
- The role and responsibilities of the Senior Information Risk Owner (SIRO) and Information Asset Owners (IAOs) in providing assurance that information risk is being managed effectively.
- The role of Information Asset Administrators (IAAs) e.g. operational staff, to assist IAOs within larger organisations.
- What is meant by an organisation’s information assets and how risks to them should be identified and managed.
- The key to successful information risk management.

Assessment

Attempt **all** of the following **12** questions, and check with your IG lead whether your responses need to be recorded and logged.

Question 1: Predictable information risk is generally a product of which two factors? Select **two** or **more** options from the answers listed below.		
A	Cost	
B	Threat	
C	Media interest	
D	Vulnerability	
E	IT failure	

Question 2: Complete the sentence: The recommended approach to information risk management is that it should... Select **two** or **more** options from the answers listed below.		
A	Be comprehensive	
B	Take full advantage of existing authority and responsibility structures	
C	Associate tasks with appropriate management levels	
D	Avoid unnecessary impacts on day to day business	
E	Ensure that all the necessary activities are discharged in an efficient, effective, accountable and visible manner	

Question 3: Which of the following are objectives of information risk management? Select **two** or **more** options from the answers listed below.		
A	Eliminating all identified information risks	
B	Identifying risks	
C	Improving press relations	
D	Meeting legal and statutory requirements	
E	Reducing risk	
F	Protecting heath and care organisations and their service users from adverse consequences	

Question 4: Who is primarily responsible for cultivating a practice of protecting, valuing and correctly using information for the benefit of health and social care and its service user? Select **two** or **more** options from the answers listed below.		
A	CEOs	
B	SIROs	
C	IAOs	
D	The IT Department / supplier	

Question 5: Incidents can never be entirely avoided so what should the SIROs goal be in terms of the corporate management of information incidents? Select **one** option from the answers listed below.		
A	The SIRO needs to investigate every incident personally	
B	The SIRO should ensure that the organisation never gets blamed for incidents in the media	
C	The SIRO needs to ensure that all staff are aware that they will be dismissed if they are involved in any sort of incident that embarrasses the organisation	
D	The SIRO needs to establish a corporate culture in which, when things do go wrong, people are confident enough to share the lessons learned	

Question 6: How regularly should IAOs undertake information risk assessment reviews? Select **two** or **more** options from the answers listed below.		
A	Whenever other work pressures permit	
B	Ideally, every three months for important assets	
C	At least annually to provide the SIRO with assurance that information risks are being managed effectively	
D	Whenever an incident occurs, no matter how trivial	

Question 7: Who should ensure that procedures for authorising use of an information asset are both robust and implemented? Select **one** option from the answers listed below.		
A	The Caldicott Guardian	
B	The Head of IT (eHealth, ICT or equivalent)	
C	The IAO	
D	The SIRO	

Question 8: The responsibilities of an Information Asset Owner include? Select **two** or **more** options from the answers listed below.		
A	Undertaking regular risk assessment reviews for all ‘owned’ information assets	
B	Escalating risks to the SIRO where appropriate and making the case where necessary for new investment to secure ‘owned’ assets	
C	Carrying out privacy impact assessments for all new projects that meet the criteria specified by the Information Commissioner	
D	Providing an annual written assessment to the SIRO for all assets ‘owned’ by them	

Question 9: Which roles might help an IAO to conduct an information risk review? Select **two** or **more** options from the answers listed below.		
A	Information Security Officer	
B	Caldicott Guardian	
C	Local journalists	
D	Records Managers	
E	Operational staff working with an information asset	

Question 10: Which of the following are information assets or components of such? Select **two** or **more** options from the answers listed below.		
A	Personal information	
B	Software	
C	IT hardware	
D	System documentation	

E	The skills and knowledge of a system administrator	

Question 11: It often makes sense to group information assets. Which of the following might be an appropriate information asset group? Select **one** option from the answers listed below.		
A	All of the information assets that Board / senior management team members use in their day to day work	
B	A pathology system, the organisation’s information security policy and the Records Management Department	
C	All staff and patient records	
D	An IT system, its system documentation, the data held within it and the skills of staff who administer it	

Question 12: Where time and resources are constrained, which of the following information assets should be given priority in respect of safeguards and controls? Select **two** or **more** options from the answers listed below.		
A	IT hardware and software	
B	Contracts and agreements	
C	Patient and staff personal information	
D	Business and continuity plans	