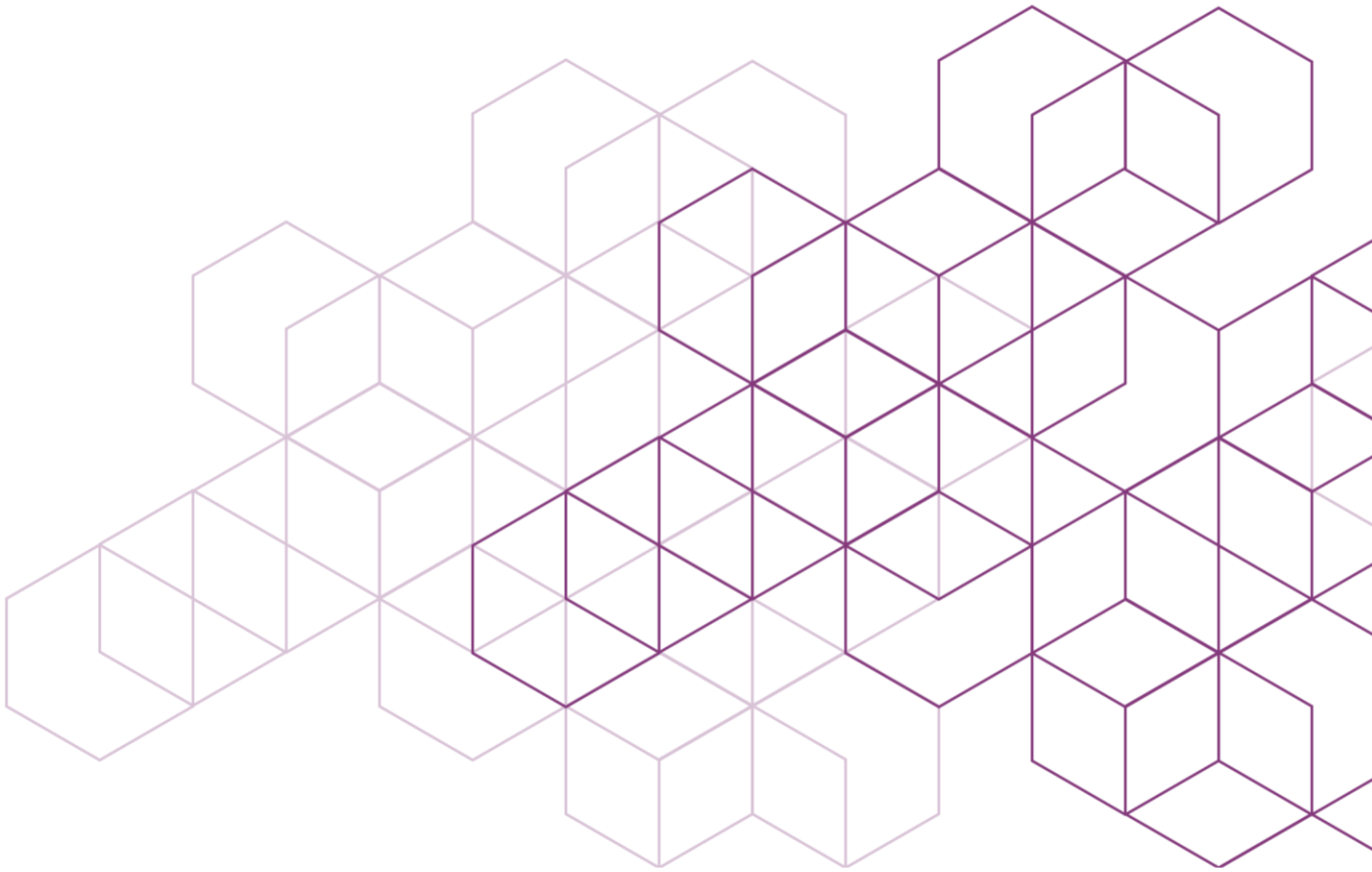
Government Digital Service

Government Skills

Information Asset Owner

Training Handbook



Government Digital Service

Government Skills

Contents

Government Digital Service

Government Skills

Introduction:

Information Asset Owner Training Course

This training course is designed for Information Asset Owners, providing essential guidance and support to help you carry out your responsibilities and daily activities. Your leadership will help your organisation understand the information that it holds, principally to ensure accountability for both personal and business-critical information. Additionally, you will play a key role in ensuring compliance with information management and legal obligations, such as data protection.

Your role is vital in identifying and understanding business-critical information assets. By ensuring these assets are used safely and managed responsibly, you will enable better, risk-based, business-led decisions that protect and maximize the value of the information assets within your organisation.

Learning Outcomes

On completion of this course, you will be able to:

- Understand and describe the requirements of your role and daily tasks as an Information Asset Owner
- Manage your information assets, to ensure that an accurate Information Asset Register is maintained and reviewed on a regular basis
- Describe your role in relation to the wider information management functions within your organisation
- Recognise the importance of your role in contributing to Knowledge and IM governance, data protection, cyber and information security, and legal obligations
- Describe the evolving threat and risk landscape, identify risk to information and how to prevent breaches
- Apply knowledge to help improve culture and instil good information handling practices within individual teams
- Provide assurance that information is managed appropriately and make key decisions on sharing, retention, and disposal of information

Government Digital Service

Government Skills

Chapter 1. Information Asset Owner

Overview - Information Asset Owner Training

Welcome to this training course for information asset owners.

Your role is crucial in ensuring your organisation can effectively identify and understand the information it holds and shares.

It also helps safeguard and manage the information that the government needs to deliver services or carry out its strategic objectives.

As an Information Asset Owner, you are accountable for information assets and you have the responsibility to understand what information is held by your organisation, how business critical the information is to your organisation, the value and sensitivity of the information, and where information is held or stored and who has access to it.

Your role interconnects with multiple functions including knowledge and information management, security and data protection, cybersecurity, digital, risk management and governance.

Information is a business asset. It must be handled and managed effectively.

You have the responsibility to understand the landscape and risks associated with information assets and to ensure the appropriate action is taken to protect them.

Your role enables your organisation to make critical decisions on how to optimise, share, store and use the information that it is accountable for.

This training course will help you navigate the key areas of your responsibilities and ensure you have the confidence to undertake your role.

In addition to this training, there may be local policies and practices in place which you will need to be aware of.

What is an Information Asset Owner?

Information Asset Owners (IAOs) are senior individuals who have strategic oversight of how their organisation manages personal and critical business information, ensuring effective exploitation of information. IAOs provide accountability for driving delivery of good practice including strategic management of information, in compliance with legal obligations, policies and standards, to reduce information risks. IAOs form part of their organisation's information governance structure and should have access to the Accounting Officer. The IAO would usually be a Senior Civil Servant.

Government Digital Service

Government Skills

Why do we need Information Asset Owners?

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. Information Asset Owners provide leadership in driving a holistic and coordinated approach for the exploitation of information assets through delivery of knowledge and information management governance, compliance with legal, regulatory and policy requirements, through effective information asset management.

Information Asset Owners:

- Are accountable for the effective and ethical use and handling of information assets within their area of responsibility
- Support best practice for information governance across the organisation
- Ensure management of information assets in compliance with legislation and the organisation's policies and standards
- Assign Information Asset Managers to the organisation's assets
- Identify, understand and mitigate risks associated with information assets
- Receive assurance from delegated teams that those responsibilities are being effectively performed
- Provide formal reporting on information assets to the relevant organisation board level
- Ensure security measures are in place when sharing information
- Understand whether a delivery partner or supplier has access or handles information assets
- Ensure staff are trained and aware of their responsibilities in protecting and managing information that they access

Role and Responsibilities – what activities do IAOs need to do?

The role of Information Asset Owner comes with a variety of responsibilities and requirements in support of leading a culture of best practice across the organisation. This includes core activities that are essential for the effective management and protection of information assets, to ensure their value is fully utilised, contributing to the organisation's success and resilience.

The priorities and activities for Information Asset Owners, working with their Information Asset Manager and teams:

- **Accountability:** Maintaining clear accountability within the organisation, for the management and protection of information assets. This includes documenting responsibilities, monitoring performance, and reporting on the status of information assets. IAOs oversee decisions on use, transfer, access controls and incident reports, providing strategic direction for information assets. Accountability cannot be delegated.
- **Identification and Categorising:** Identification and categorising of all information assets within the domain. This involves determining what constitutes an information asset and categorising it based on its importance, sensitivity and usage.
- **Valuation:** Assessing the value of information assets to the organisation. The identification of the highest value assets and applying appropriate additional security controls. This helps in prioritising resources and efforts towards the most critical assets.
- **Risk Management:** Identifying and mitigating risks associated with information assets. This involves evaluating risks, implementing mitigation measures, and monitoring for any emerging risks. Ensure information assets are managed in line with the organisation's risk appetite.
- **Security:** Implement and oversee security measures to protect information assets from unauthorised access, breaches, and other threats. This includes setting access controls, and other security protocols, including conducting regular security checks.
- **Information Asset Register review**: Maintain an accurate and up-to-date Information Asset Register. This includes documenting details such as the asset's location, owner, and classification and including any new assets or changes in status.
- **Data Usage & Access**: Monitor the usage, make decisions on use, transfer, and access controls. Ensure that where needed, data sharing agreements and memorandums of understanding are in place to ensure they are being used appropriately and in compliance with legal and organisational policies.
- **Collaboration:** Working with other stakeholders, such as Digital, Security, Legal, and Compliance teams, to ensure a holistic approach to information asset management. This collaboration helps in sharing insights and aligning efforts and resources.
- **Compliance**: Reviewing and ensuring that the management and usage of information assets comply with relevant regulations, policies and standards and making necessary adjustments when needed.

- **Reporting:** Providing regular reports on the risk status, usage and protection of information assets. This includes documenting performance, compliance, and any issues or incidents.
- **Breach Reporting:** Engage in the management of data breaches and serious security incidents relating to information assets, along with the Data Protection Officer and Cyber and Security Teams.
- **Efficiency:** Streamlining the management of information assets to ensure they are used efficiently and effectively. This involves optimising processes, tools, and resources to support business operations and decision-making.
- **Disposal:** Oversee the proper disposal of information assets that are no longer needed. This includes ensuring that disposal methods comply with legal, security and regulatory requirements.
- **Continuous Improvement:** Continuously seek ways to improve the management and protection of information assets. This involves staying up-to-date with the best practices, technologies, and regulatory changes.

These activities ensure all information assets are identified, and an accurate information asset register is maintained to understand:

- What information is held?
- The sensitivity and risks associated and ensure they are managed appropriately
- Who has access and why?
- How information is stored, used, moved, and shared

Overall, the IAO must understand the risks associated with the information assets they own and be satisfied that measures are in place to appropriately safeguard them. Ensuring full use of information within the legal, regulatory and policy requirements, ultimately providing assurances to the relevant internal information governance boards (or equivalent).

You have completed this chapter

Please start chapter 2

Chapter 2. Information Asset Manager

Government Digital Service

Government Skills

What is an Information Asset Manager (IAM)?

An IAM is a delegated role working on behalf of the IAO, with regular responsibility for the proper management of information in their business area.

While some tasks require direct involvement from the IAO, others may need only IAO oversight and can be delegated to IAMs who can manage the information assets. Nonetheless, accountability remains with the IAO and cannot be delegated.

The role is flexible and may be implemented differently in organisations. Most IAMs will perform the role in addition to existing duties.

What is the role of the Information Asset Manager (IAM)?

The IAM provides assurance to the IAO that information assets are being managed appropriately, and associated risks are understood and mitigated as needed within individual business areas. IAMs should ensure the protection of data and information that the organisation holds, ensuring information is handled and shared securely with colleagues, other government departments and suppliers.

The IAM implements the IAO decisions on use, transfer and access controls for the asset. The IAM will review and provide challenges on access and movement of their assets and understand the risks associated with their assets.

How do I appoint an IAM?

Each organisation will have their own process for appointing IAMs. Some will provide a letter of appointment for new IAMs and have minimum requirements and grades for IAMs. The requirements for who is appointed as an IAM will depend on the size, complexity and nature of the information asset that is being managed on behalf of the IAO.

The IAO should help identify IAMs and develop the best approach for their organisation. Once appointed, IAMs must undergo training to ensure that they are fully equipped to undertake all the responsibilities of their role.

Role and Responsibilities – what activities do IAMs do?

The IAM has daily operational responsibility and liaises directly with teams or directorates, or those handling information assets. IAMs support the IAO by providing hands-on knowledge and duties associated with the management of information assets.

The IAM role is crucial and requires knowledge in a range of areas to take the lead in promoting good IM practices - The main activities of the IAM include:

Management of information assets:

- Working closely with and for the IAO
- Build relationships with those creating information assets as part of their work
- Identifying and understanding the information assets used in business areas
- Acting as a point of contact for queries and requests involving information assets
- Understanding the importance for security measures to protect information
- Identifying business-critical and sensitive assets and risks associated with them
- Identifying risks to aggregated data and information
- An ability to assess gaps in the IAR and make improvements where necessary
- Controlling access to the assets, based on business needs
- Providing advice and implementing requests to move or manipulate content
- Identifying risks and opportunities with the asset

Maintenance of an Information Asset Register (IAR)

- Ensuring Information Asset Registers record all information assets used in business areas, including adding new assets
- Implementing Information Asset Register assurance activity
- Identifying and mitigating risks to assets and ensuring they are captured
- Undertaking compliance checks of electronic and hardcopy information
- Regularly providing assurance to the IAO that the information assets are managed effectively and in accordance with relevant legislation
- Escalating concerns regarding the highest risk assets and when to apply additional security controls
- Having a basic knowledge of, and collaborating with, other related roles, for example, Knowledge and Information Management, Governance, Data Protection, Cyber, Security, and Legal

- Having confidence in raising issues or escalating concerns to the IAO
- Ensuring Data Protection Impact Assessments (DPIA) are completed when required
- Ensuring staff who process personal data undertake relevant training

You have completed this chapter

Please start chapter 3

Government Digital Service

Government Skills

Chapter 3. Information Assets

What is 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 efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles.

An information asset can be a single document or a large data set. It could be held electronically or on paper and it could include personal or non-personal data.

An information asset may be critical to the achievement of the Governments strategic objectives or support the completion of key tasks within an Information Asset Owner's area of responsibility.

How to determine your information assets?

An information asset is a body of information that may have one or more of these characteristics:

- It has value to the organisation
- It supports a business or operational process (business-critical)
- It enables policy development or decision-making
- It enables your organisation to keep the public or ministers informed
- There is risk associated with the information
- It contains sensitive or personal data
- It is shared with partners
- It has longevity and a lifecycle
- Its loss, compromise or unavailability when required will be harmful to a business's reputation or prevent the business from delivering its business outcome
- It will have an impact on resources if it is replaced (cost, skills, time etc.)

Information assets are the business-critical bodies of information within your organisation, the kind of information that, if it became lost, stolen, corrupted, modified, or unavailable, it would cause significant impact to your organisation's reputation and/or delivery outcomes.

An information asset is not a system or database. The information that is held on the system or database is the information asset and there may be multiple information assets held in a single system.

Information assets that are hosted or handled externally by a third party are still under the ownership and management of the organisation and therefore the IAO is accountable for those information assets within their area of responsibility and must ensure they are handled securely.

Information assets should be grouped based on content and consideration should be given to their business needs, not their technical requirements.

Examples of information assets

Information assets could be:

- Collection of citizen or patient records
- Local database containing specific information such as payments or budgets
- HR files and folders which include personal data
- Set of data subject records on a system – personal data sets being routinely managed/used
- Policy formulation documents and communications related to a subject
- Database of related information e.g., Financial or Commercial
- Statistical information e.g., group of linked spreadsheets
- A collection of documents on a subject for a specific purpose regarding business operations
- A set of administration files where your organisation has lead responsibility
- Information required to be maintained by law

Information assets are not:

- Physical Hardware such as laptops/desktops
- IT systems can host different types of information assets, or process information for different business purposes

Information Assets

All information associated with a specific project (such as reports, digital records, documents, images, emails, photo images, sound /voice recordings and any other form of digital records) can be grouped together and treated as a single asset, as they have similar definable content and the same value, business risk and lifecycle.

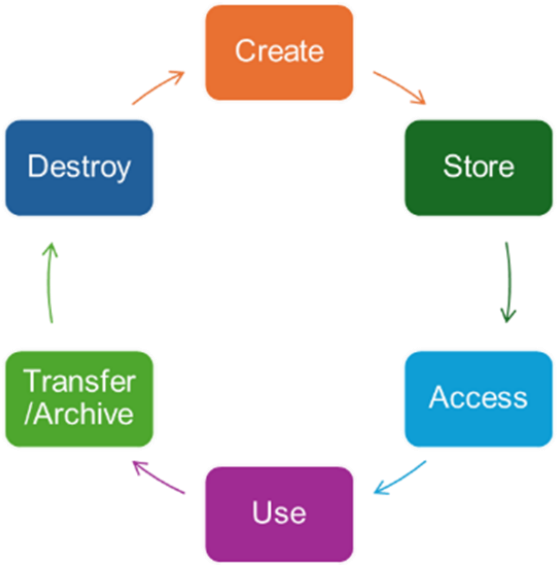
A list of contacts held on a database must be grouped as a single asset. The usage will have a single business purpose and joint risks associated with privacy and storage of personal information. Therefore, each entry does not need to be treated individually and can be considered jointly as a single information asset.

Where an information 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 security level required. Consideration also needs to be given to differing retention periods, handling instructions and descriptors.

Information Lifecycle

Information lifecycle management is the consistent management of information from creation to final disposal. It is comprised of strategy, people, process, and technology to effectively manage information which, when combined, drives improved control over information assets within the organisation.

The lifecycle of an information asset encompasses several stages: creation, storage, access, use, transfer/archiving, and eventual destruction.



A diagram of the Information Lifecycle process

Each phase should be managed effectively to ensure the asset is protected and handled securely (with integrity, confidentiality, and availability).

Create: During the creation phase, data is generated or acquired, requiring classification based on sensitivity.

Store: It is then stored securely, using appropriate systems that protect against unauthorised access or loss.

Access: Controlled access ensures that only authorised individuals can retrieve or modify the asset, supporting accountability and compliance.

Use: The use phase involves leveraging the asset to support business operations, decision-making, or service delivery, while maintaining its accuracy and relevance.

Transfer/Archive: During the lifecycle it is crucial to implement measures to minimise risk, ensure regulatory compliance, and maximise the value of information assets throughout their existence.

Destroy: When the asset is no longer actively needed, it may be transferred or archived for long-term retention, ensuring it remains retrievable and protected.

Records Management

Storing, and naming information assets

Government organisations must maintain accurate administrative records ensuring that they are accessible for public review. Information should be managed from its creation to its disposal. Business-critical information necessary for understanding the administration of an organisation must be properly saved and stored as corporate records. These records are maintained in registered files.

Good information governance involves:

- Establishing common naming conventions for files and documents to ensure better access and understanding of information assets
- A structured system for naming files, makes them easy to identify and organise

It ensures consistency for describing documents' content, helping to identify relationship to other files, saves time searching, and reduces risk of data loss or misplacement. It also aids in identifying assets for the information asset register (IAR).

Storage

When assets reach the end of their useful life, organisations must consider disposing of information in line with their retention and disposal schedule. Where information forms a record, then consideration needs to be given to archiving and the Public Records Act 1958. The Act mandates that public authorities are responsible for selecting which records are permanently valuable and should be preserved. Records selected for permanent preservation are transferred to the National Archives (TNA). Any information that does not warrant preservation must be securely destroyed to prevent data breaches or misuse.

Records can be in any format. For example, email, paper, electronic, sound recording. Records can be a single document or a group of documents with a common unique theme. It is the content that makes a document a record, not the format.

Corporate records

Corporate records must be stored in registered files to maintain information integrity and document decision-making, policy development, expenditures, and support any legal challenges. Staff must record their decisions, advice, and actions, especially those classified as corporate records. The information author/owner should ensure that all information is handled in accordance with the organisation's Information Management Policy and supporting guidance.

Documents that have been identified as an important corporate record must be kept as follows:

Registered Files – this is the formal paper-based system used to control and manage the most significant corporate records, which include those considered significant in terms of public interest, spending, or have a potential national impact.

E-Registered Files – these are electronic versions of a paper registered file. If used, there is specific guidance these are to be kept and maintained to ensure the integrity of the information is preserved.

Corporate Record Boxes – these are used for bulky records that would otherwise be held in a registered file, for example finance, legal, estates and procurement documents

Your organisation will have their own records management and storage process in place. Please check with your organisation DRO for further information.

You have completed this chapter

Please start chapter 4

Government Digital Service

Government Skills

Chapter 4. Information Asset Registers (IAR)

What is an Information Asset Register - overview

The Information Asset Register (IAR) is a useful tool providing an IAO with a comprehensive overview of the organisation's information assets. It serves as an inventory to manage and assess risks by mapping information assets to business needs. How assets are recorded and the information captured may vary in different organisations. The IAR is typically maintained electronically (such as on a SharePoint site, M365 List or Excel) and is completed or reviewed regularly by the relevant IAM within their respective business areas. The organisation can have a single IAR for the whole organisation, or one per IAO.

What are the contents of the IAR & scope?

The IAR includes details such as the name, description, data/business ownership, purpose, classification, sensitivity, associated risks, and whether personal data is contained within each information asset. The IAR includes all information assets held in hardcopy, digital files and information stored in databases, and it specifies classification, access permissions, the lifecycle of information assets and describes measures in place for protection of the assets.

Internal IAR:

- Reviewed and updated regularly (such as biannually or annually)
- Ownership of Assets
- Name and description
- Access and sharing
- Security classification and controls
- Review and retention
- Business value and risk
- Personal data
- Public register mapping

Public IAR

- Updated annually or as required
- Published on gov.uk
- High level consolidated view of assets held
- Name and description only

Government Digital Service

Government Skills

Why is the IAR important?

An IAR helps the IAO fulfil their duties, providing a detailed view of the organisation's information landscape. It enables the organisation to implement best practices around information governance, legal and regulatory compliance, and HMG policies. It is essential the IAR is up to date and accurately reflects the information assets held by the IAOs area of responsibility.

The IAR ensures implementation of the following:

- **Legal compliance** - The ICO advises all government bodies to maintain an updated IAR, including documenting the basis for all personal data processing activities and the Record of Personal Processing Activity (RoPA) to comply with UK GDP
- **Responding to Subject Access Requests** - Knowing what personal data is retained and where it is located allows the organisation to manage requests from individuals for access to their information more efficiently in compliance with UK GDPR
- **Responding to FOI and EIR requests** – Supporting requests for information in line with the Freedom of Information Act 2000, and Environmental Information Regulations 2004
- **Policies & guidance** – The Cabinet Office advises government organisations to use an IAR for appropriate management of their information assets. The organisation is expected to have relevant information governance policies. Use of the IAR helps ensure that required compliance is met
- **Information asset review & identification** – IARs help an IAO undertake an assurance review; understand and locate valuable and sensitive information for secure and effective use and support with business outcomes and decision making
- **Risk Assessment** – IARs help identify the assets with the highest risks associated with the information, confirming where to focus efforts on implementing controls
- **Access control** – IARs ensure information assets are monitored and access to them are applied correctly, based on the 'need to know' business requirements
- **Data Sharing / 3rd Parties** – IARs enable the organisation to easily identify data sharing, both internally and externally and highlight third-party data processing. This may include details of any agreements or contract clauses which specify what data can be shared and how

- **Supports Strategy and Policy –** IARs provide a comprehensive understanding of the organisation's information assets which can significantly enhance exploitation, usage and development of policy and strategy
- **Knowledge Management** – acts as a central repository identifying duplication of assets and ensures enforcement of information retention schedules

Who is involved in the register?

The IAO is the senior leader accountable for ensuring that their area of responsibility within the organisation regularly conducts activities to develop, maintain, and review the IAR. This living document is maintained by designated Information Asset Managers authorised by the IAO.

- **Information Asset Manager** – is responsible for the direct management of information assets. Oversees asset entries in the IAR and addresses internal inquiries. Conducts regular reviews and updates of IAR entries to add, amend, or remove assets
- **Assurance and Compliance team** - various roles and responsibilities are involved across individual organisations, contributing to the IAR, for example, validation of entries, obtaining approval for and publishing the public information asset register; and providing support to IAOs and IAMs throughout the review process
- **Technical Teams** (Knowledge and Information Management, Digital and Data, Cyber, Security – roles vary by organisation):
    - understand the platform/systems containing information assets
    - evaluate capabilities and limitations of platforms/systems
    - provide advice on access control and audit logs if requested
    - implement content movement/manipulation requests
    - identify technical risks and opportunities related to stability, longevity, effectiveness, and cost of hosting assets

The IAO must ensure that all delegated responsibilities are understood and that all duties are undertaken for a comprehensive assurance process. This requires full collaboration and coordination between the various disciplinary and technical teams.

How to maintain the register

IAMs are part of the team that manages information assets on a day-to-day basis, from granting access to assets for new joiners to removing access from leavers.

Other responsibilities required to maintain the IAR include working with other teams to keep it accurate and updated as required, in advance of the formal regular review and assurance period:

- New assets & risk identified are included in the register
- Information assets no longer required etc. archiving/deletion

Please see your organisation's guidance for specific instructions on how to remove information assets from your IAR or seek guidance from the Departmental Records Officer (DRO).

Review cycles

IAOs are responsible for establishing regular review processes internally, to verify the composition of information assets, ensuring alignment with core elements of information security, legislation, and compliance. As an IAO, it is important that you understand your organisation's process for recording changes relating to information assets.

The review process helps to assess whether individual business areas are managing information assets appropriately aligned to information governance policy and procedures, supporting Information Asset Managers in fulfilling their roles and responsibilities.

Organisations need to establish a formal process with relevant assurance teams, to complete the regular review and assurance process.

The review should be conducted biannually or at least annually, providing formal reports on information asset status.

Elements of the assurance process should include checks on the following (this list is not exhaustive):

- All information assets that the IAO is accountable for, how and where it is stored and the business activity it supports
- Who is accessing the assets and why, and what are the risks and risk ratings
- Under the UK GDPR, a record of processing activities (ROPA) is in place
- Ensure that personal information is not unlawfully exploited

- Record the asset classification; sensitive assets and personal data should be identified
- Understand what physical and organisational measures are in place to ensure that the information held in your assets is processed and protected properly
- Ensure the asset is fit for purpose and used ethically
- Ensure that information is only kept for as long as it is required to carry out business, or to comply with statutory responsibilities and legislative requirements
- Ensure compliance with information sharing agreement requirements
- That retention schedules are applied, and end-of-life information is considered for transfer to the National Archives or securely destroyed when there is no further requirement for it, helping compliance with Public Records Act obligations
- Record in what format assets are held i.e. in systems, digital electronic and hardcopy information – and how they are controlled, retained and exploited
- Ensure a record of breaches and incidents is kept & maintain incident management reports relating to the asset
- A record of information assets handled by third parties/suppliers, risks – controls & measures in place for protection
- Ensure guidance & training is available and undertaken by IAMs
- Ensure measures are in place so that all staff are aware of their responsibility to handle information securely
- Be aware of business continuity and emergency plans to reduce or prevent interruptions to business activities due to significant disruptions to information assets

Scenario 1

In the event of data being stolen by an attacker, we need to be able to inform people what information could have been lost. The IAR would be used to provide that information.

Your organisation has suffered a targeted cyber-attack, potentially involving ransomware or data theft. Systems that contain sensitive personal information about colleagues, including HR databases and payroll systems, have been compromised.

The incident response team requests a copy of the IAR to quickly assess the scope of the breach. Upon reviewing the IAR, the team identifies that bank details, home

addresses, National Insurance numbers, and emergency contact information may have been accessed.

The IAR helps pinpoint which systems were affected, the owners of those assets, and the sensitivity of the information, enabling a rapid response

- The organisation is able to:
    - Notify affected colleagues promptly
    - Provide guidance on steps to protect themselves (for example, contacting banks, monitoring credit reports)
    - Achieve legal obligations under UK GDPR and report the breach to the Information Commissioner's Office (ICO) within the required timeframe

The scenario demonstrates the importance of a well-maintained IAR in:

- Supporting rapid decision-making during incidents
- Ensuring regulatory compliance
- Minimising the reputational damage and personal harm for such incidents

You have completed this chapter

Please start chapter 5

Chapter 5. Legal & Policy requirements

Legal requirements

As an IAO, you must ensure that your area of responsibility complies with relevant legal, regulatory and policy requirements covering information governance. This includes managing and safeguarding information and providing public access to information where appropriate.

This includes the following:

- **Freedom of Information Act 2000 (FOI)** – and Environmental Information Regulations 2004 (EIR) – This legislation gives citizens the right to request recorded information from the Government and other public authorities. If a member of the public wants to obtain information that a public authority holds about themselves (personal data) they can submit a Subject Access Request (SAR) under the UK General Data Protection Regulation (UK GDPR)
- **Public Records Act 1958** – A legal framework for preservation, management, and access to public records in the UK. The 20-year rule is when government

records selected for permanent preservation are transferred to The National Archives and made publicly available

- **The Civil Service Code** – A formal document that constitutes part of the Terms and Conditions of employment for all Civil Servants. It sets out the core values and standards of conduct that Civil Servants are expected to uphold in their daily responsibilities, ensuring they act with integrity, honesty, objectivity, and impartiality
- **Official Secrets Act 1989** – The act to prevent espionage and unauthorised disclosure of official information, safeguarding national security. The Act addresses offences related to spying, sabotage, and related crimes. Including the unlawful disclosure of government information by current and former employees of the security services and Crown Servants
- **Computer Misuse Act 1990** – The act criminalises unauthorised access to computer systems and data, as well as damaging or destroying them. Computer abuse includes activities such as cyber-bullying, hacking and identity theft
- **Data Protection law (UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data (Use and Access) Act 2025).** The Data (Use and Access) Act received Royal Assent on 19 June 2025, and changes some of the requirements. For the latest information please see the ICO guidance.

UK GDPR and the Data Protection Act

UK GDPR and Data Protection Law are two pieces of legislation that together govern how organisations must protect personal data to safeguard individuals privacy.

They also detail how personal information should be used and handled by organisations.

What is Personal Data?

Personal data is any information about a living person, also known as the data subject, which can be used to identify them either by itself or when combined with other information.

Some more personal data, including criminal offence data may be classed as special category data which requires additional stipulations under the Data Protection Act.

All requirements of UK GDPR are based on 7 principles. Implementing these principles will help organisations to comply with the Data Protection Law.

The 7 data protection principles are:

- **Lawfulness, fairness, and transparency**: there must be a valid legal basis for processing personal data and organisations must be open and honest about their intended processing
- **Purpose limitation**: Personal data should be collected and processed only for specified, explicit, and legitimate purposes
- **Data minimisation**: Only the minimum amount of personal data needed to fulfil your purpose should be collected and processed
- **Accuracy**: Personal data should be accurate and kept up to date, where necessary
- **Storage limitation**: Personal data should not be kept for longer than necessary for the purposes for which it was collected
- **Integrity and confidentiality** (security): Personal data should be processed securely using appropriate technical and organisational security measures
- **Accountability**: Controllers must be able to demonstrate that they are complying with the data protection principles

The proper handling and processing of personal data is a legal obligation. Failure to adhere to these obligations could result in a public reprimand, financial penalties,

reputational damage and operational disruption. Your own organisation will have a Data Protection Policy. Check with your Data Protection Officer (DPO).

Data Protection Impact Assessments (DPIAs)

Privacy by design is mandated by UK GDPR. It involves integrating data protection into system design from the start, rather than adding it later. A DPIA should be started early in the life of a project to help ensure privacy is considered as part of system design. All new information assets containing personal data or changes to the handling of personal data must be assessed via a DPIA.

A DPIA analyses, identifies, and mitigates data protection risks in projects. Under UK GDPR, you must do a DPIAs before you begin any type of processing activities likely to result in a high risk to individuals' rights and freedoms. Not conducting a DPIA could lead to enforcement action. If in any doubt do a DPIA to ensure compliance and encourage best practice.

A DPIA acts as a checklist.

- It evaluates privacy impacts and ensures robust information security
- It assesses risks such as confidentiality threats that could potentially damage individuals or the organisation's reputation if information is disclosed in error

For further information on DPIA visit the ICO Website.

Record of Processing Activities (ROPA)

Under Data Protection legislation, data controllers (usually an organisation) are required to maintain a Record of Processing Activities (ROPA). This demonstrates accountability to ensure personal data is processed in accordance with the law.

A ROPA is an internal document that details an organisation's activities for processing personal data. It provides a summary of what personal data is collected, how it's used, who it's shared with, and what security measures are in place. The IAO can use the ROPA to help support them in their role, including understanding the risks and

mitigations that are in place for their information and what the purpose of data processing activities are.

Further information on ROPA can be found on the ICO website.

Data-Sharing Agreements

A data-sharing agreement facilitates the exchange of personal data between two separate controller organisations. It outlines the roles of the parties, sets out the purpose of the data-sharing, covers what happens to the data at each stage and sets the standards for protecting and handling the data. IAOs may be asked to approve new data sharing agreements involving their information assets.

Data-sharing agreements help an organisation to demonstrate that it is meeting its accountability obligations under the UK GDPR. Government departments and certain other public bodies may enter a memorandum of understanding with each other, which will include data-sharing provisions and will fulfil the role of a data-sharing agreement.

When information is shared with a third party there may be an associated security risk to the information, particularly when transferring data.

- Data-sharing requires a legitimate business purpose
- Share only the essential data
- The recipient must have a 'need to know' and proper security measures for handling data according to its classification must be in place
- Data must be transferred securely, meeting minimum security standards set by the classification

What are the benefits of information sharing agreements?

An information sharing agreement clarifies roles and documentation of compliance.

The agreement must outline the following:

- Identify the parties involved in the agreement
- What is the purpose of the data-sharing initiative?
- What other organisations will be involved in the data-sharing activity?
- What data will be shared?
- What is the legal basis for sharing?
- Does the data include special category data, sensitive data, or criminal offence data?

- Have you considered rights and access?
- What information governance arrangements should be considered for implementing?

Your individual organisation will have a process in place for data sharing agreements. Please check with your Data Protection Officer.

For further information on Information sharing agreements visit the ICO website.

Policy Requirements

As an IAO you are accountable for ensuring staff handling your information assets are aware of their obligations regarding secure handling of information, including reiterating the need for staff to complete the relevant training courses. There are specific internal policies and procedures to ensure staff understand their responsibilities and the expectations placed upon them.

As an IAO it is important that you know what your organisations policies are on handling information to effectively minimise risks, in addition to the policies listed below:

1. Acceptable use Policy (AUP)

The AUP helps to ensure that all employees (users) with access to the organisation's information assets and systems understand their responsibilities for the appropriate and secure use of the organisation's information technology resources (all equipment, including hardware, software and communication channels such as telephony, social media, video, email, instant messaging, internet, and intranet).

2. Social Media Policy

The social media policy outlines employees' responsibilities for the secure use of social media, both at home and at work. It specifies the expected behaviour of employees when engaging on social media platforms. For instance, it includes rules against posting official and sensitive information, to prevent leaks and to ensure security. The policy also aims to prevent slander, defamation, and minimise reputational damage to the organisation while encouraging employees to act responsibly and safely.

3. HMG Security Classifications Policy

The Government Security Classifications Policy provides an administrative system for HM Government and its partners to protect information assets against prevalent threats. Classification is based on the potential impact of the compromise, loss, or misuse of information. The policy covers procedures for creating, sharing, and destroying information, setting the baseline security controls and behaviours necessary to protect information at each classification tier.

4. Government Functional Standard GovS 007: Security

The purpose of this government functional standard is to set expectations for protecting the government's assets (people, property and information), visitors to government property, and third-party suppliers whilst engaged on government business and citizen data.

5. Government Functional Standard GovS 005: Digital

The purpose of this government functional standard is to set expectations for the management of digital, data and technology in government to enable defined policy outcomes, improve the usability and efficiency of government services and improve the operating effectiveness of government organisations.

6. IAO guidance

The guidance for IAOs was refreshed in Autumn 2025 and contains the core activities and responsibilities of the IAO role. For further information please visit The role of Information Asset Owners (IAOs) in government - GOV.UK

As an IAO, it is important to collaborate with assurance, technical teams, security experts, and the data protection team, to ensure the secure handling of information within your organisation. Making sure you are visible and approachable to these teams, to effectively manage legal risks.

Government Digital Service

Government Skills

Scenario 2

The importance of ensuring information assets that contain personal data are deleted in line with your organisations Records Retention Schedule.

Your organisation has received a Subject Access Request (SAR) from an individual who previously worked for the organisation.

The team dealing with the Subject Access Request contacts the Information Asset Owner within the Human Resources team to check what, if any, information is still held for the individual.

Upon checking they find that the individual's personnel file is still being held even though it should have been destroyed in line with the organisation's Record Retention Schedule a number of years ago.

The information contained within the personnel folder is released to the individual. The individual requests that the organisation deletes their information as they no longer have a justified requirement to keep this.

The HR team destroys the personnel file in line with their destruction procedure and the team dealing with the SAR confirm back to the individual that this has been done.

The Information Asset Owner requests that the team managing the process for destroying personnel records is reviewed and updated to ensure this does not happen again.

This scenario highlights the importance of ensuring you know how long your information assets need to be kept for and ensure a process is in place to destroy these at the appropriate time.

You have completed this chapter

Please start chapter 6

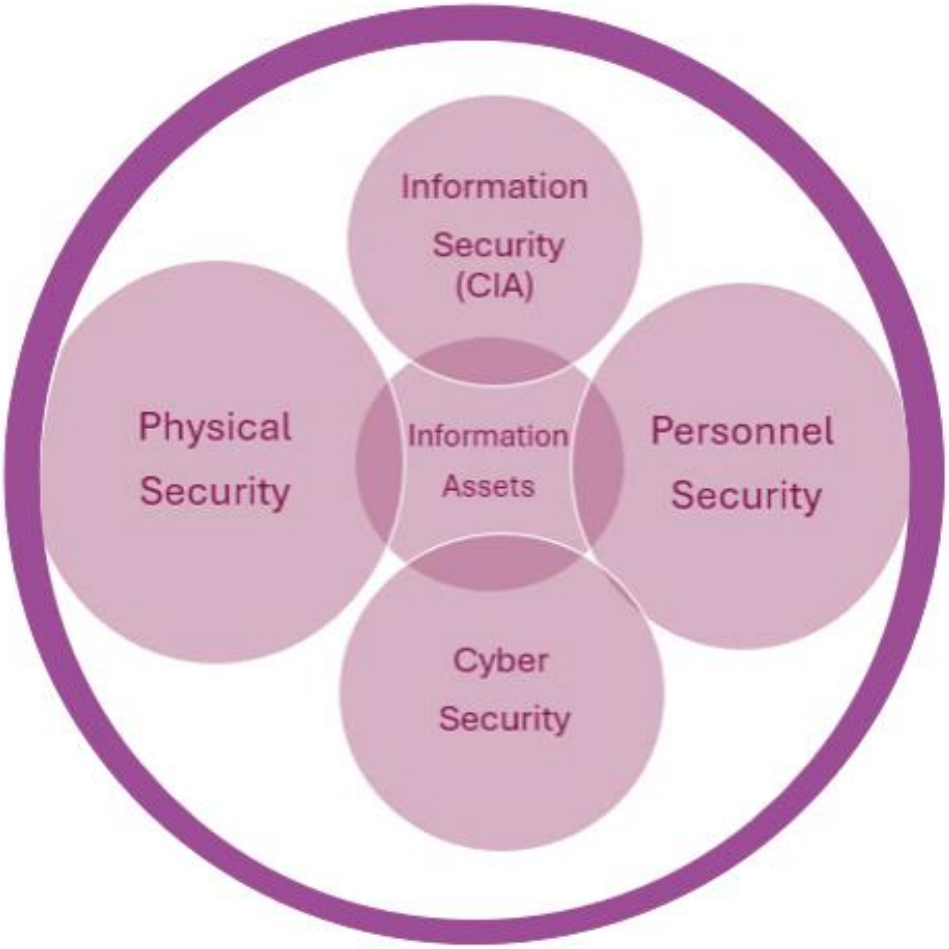
Chapter 6. Security

Holistic Security Overview

Effective information security relies on a comprehensive, holistic approach that ensures all security controls are appropriately and proportionately implemented in line with the associated risks.

Information, Cyber, Personnel and Physical Security are interrelated and dependent on each other. The most effective way to secure information assets is to use a combination of physical, information/ Cyber and personnel security measures.

For example, installing an expensive ID pass and PIN access control system for entry to an office is of little use if recruitment checks are not properly assessing who is issued with a pass.



Information Security

Confidentiality, Integrity, and Availability (CIA)

IAOs have a crucial part to play in information security, having responsibility for and authority over the information within their area of responsibility, giving them a clear view of key information risks and allowing them to formally accept, mitigate, or decline those risks, including partners.

Information security includes a combination of technical tools, policies, processes and people which are all devised to protect, prevent, detect and mitigate attacks and threats to sensitive information, whether digital or non-digital information.

Information Security is built on the core principles of Confidentiality, Integrity, and Availability (CIA):

- **Confidentiality:**
  - Protection: Ensuring that information is only accessible to authorised individuals
  - Risk: A loss of Confidentiality results in unauthorised access or disclosure of information leaks/loss of information/theft

- **Integrity**:
  - Protection: Ensuring that information remains accurate and unaltered (unless required)
  - Risk: a compromise to the Integrity of information results in inaccurate, incomplete or corrupted data and information

- **Availability**:
  - Protection: Ensuring that information is available when needed to authorised individuals
  - Risk: A lack of Availability results in authorised users being unable to access information when required

Adopting CIA principles help identify risks to assets, indicating which aspect to prioritise for protection. However, all three principles are applied for complete security coverage.

Effective information security requires a comprehensive and holistic approach, with collaboration from teams such as Digital and Data, Cyber, Security, Assurance, and Knowledge and Information Management (KIM), to manage risks effectively.

As the IAO responsible for overseeing information risk, you will receive support from these teams in identifying, mitigating, and reporting risks. It may be necessary to provide guidance or escalate matters at Board level. Additionally, extra resources might be required to implement mitigation measures and controls.

Artificial Intelligence Systems and Services

The use of an AI system or service in connection with information assets can bring valuable benefits in terms of information exploitation, knowledge and information management, productivity and process improvements.

Information Asset Ownership will become even more important as organisations need access to high-quality and well-governed information for effective AI outcomes, increasing the demand for clear ownership. IAOs should become informed about AI and how it could impact their assets.

Over time, we expect IAOs to become increasingly important in enabling the ethical, safe and explainable use of government information in AI systems.

Prior to allowing an AI service access to information, an IAO should be satisfied that the service has been assessed to ensure it does not pose a risk to information security, data quality or data privacy.

With particular consideration being given to whether:

- The AI system/service complies with the government's Secure by Design principles
- A data protection impact assessment has been carried out (if the dataset contains personal data)

Classifying and handling information

The Government Security Classification Policy provides an administrative system for HM Government and its partners to protect information assets against prevalent threats. Classification is based on the potential impact of the compromise, loss, or misuse of information. The policy covers procedures for creating, sharing, and destroying information, setting the baseline security controls and behaviours necessary to protect information at each classification tier.

The three tiers of classifications are OFFICIAL, SECRET and TOP SECRET. These classifications are determined by evaluating the value and risks associated with the information asset, including the potential impact from compromise, loss, or misuse. Higher classifications require additional security measures to prevent unauthorised disclosure or misuse of the information.

Government Digital Service

Government Skills

Cyber Security

What is Cyber Security?

Cyber security helps individuals and organisations prevent cyber-attacks. It protects devices and services, both online and at work, from theft or damage. Government organisations are increasingly targeted by cyber-attacks, to steal information, or disrupt services. Protecting information is crucial to prevent financial or reputational damage.

IAOs don't need to be technical experts but do need to know enough about cyber security to have constructive discussions with key staff, for confidence that cyber risk is being appropriately managed. An IAOs approach to cyber security should be strategic to maintain operational resilience during incidents.

- Cyber security focuses on preventing hackers penetrating your IT systems
- Cyber resilience is the ability of an organisation to protect itself from, detect, respond to and recover from a cyber-attack

Cyber Risk

An IAO needs to ensure that cyber risks to delivering business and services are identified, evaluated, and mitigated in line with the business risk-appetite.

This includes:

- Understanding the risk that cyber incidents present to delivery of the business strategy
- Ensuring that the business has adequate cyber resilience to prevent, detect and respond to cyber attacks

A cyber strategy should align with the business strategy to minimize risk, financial impact, and reputational damage. It must be integrated into risk management and decision-making processes, with all business units understanding their cyber security responsibilities.

For example:

- Technical teams secure data and systems with appropriate controls such as firewalls, Antivirus/Malware Protection etc.
- Staff should receive regular training and understand policy & guidelines
- Communications work with the IAO to prepare statements for incidents such as disruptions or breaches
- The cyber security team establishes policies to prevent unauthorised access

- Procurement teams assess cyber risk in contracts and manage supply-chain governance
- All business areas implement effective cyber security measures

Physical Security

What is Physical Security?

Physical security involves measures to protect assets such as people, government property, buildings/estates and information from threats such as theft, unauthorised access, and natural disasters. It includes securing entrances, surveillance systems, access control, secure storage, staff ID passes and other techniques to deter, detect, and respond to intrusions.

Physical security is a key area for IAOs to understand because it plays a crucial role in safeguarding both digital and non-digital assets. Physical threats such as theft, unauthorised access, or environmental damage can be just as damaging to an organisation's information confidentiality, integrity and availability.

IAOs must ensure that appropriate physical controls are in place to protect information to:

- Prevent unauthorised access to physical sites
- Protect hardware and infrastructure
- Safeguard printed information
- Environmental and disaster protection

Personnel security

What is Personnel Security?

Personnel security ensures staff safety during government business and makes them aware of their role in protecting information. It includes policies and procedures to prevent employees and contractors from misusing their access to assets.

This involves implementing measures such as pre-employment screening, vetting, security training, and access control systems to ensure that individuals are granted access to information strictly on a need-to-know basis.

Certain HMG positions or buildings require higher levels of security clearance for access to sensitive information or assets.

You have completed this chapter

Please start chapter 7

Chapter 7. Information Risk Management

What is Information Risk Management (IRM)?

IRM refers to the culture, processes and structures an organisation adopts to identify, assess, and manage potential risks to information assets. It ensures confidentiality, integrity and availability of information. The purpose of IRM is to reduce the potential for harm or loss resulting from the misuse, destruction, or unauthorised access to information.

IRM IAO Responsibilities

As an IAO, you are accountable and responsible for ensuring information within your area of responsibility can be used by your organisation to achieve its objectives. Both accidental and deliberate wrongful disclosure can harm the organisation's reputation and hinder its ability to function. Managing information risk to minimise the likelihood of staff errors or intentional misuse is a crucial responsibility. This includes preventing information loss from internal/external threats, especially during information transfers, movements, or periods of business change.

Risk Assessments

A risk assessment assesses the effectiveness and efficiency of measures to protect assets, considering policies, regulatory constraints and business objectives.

Information assets have risks such as loss, theft, unauthorised access, leaks, and corruption. Asset identification is the foundation on which all risk management is built. It is critical to identify the different forms and classifications the information may take, for example:

- Verbal Speech - briefings, meetings, VTC
- Hardcopy documentation - meeting minutes, personnel files, briefing notes, anything that is printed
- Digital - anything processed and stored on digital systems

It is also critical to identify the following:

- The people who should have access to an information asset
- The people who are responsible for managing the assets/platforms that process, store or transport information assets

- The systems used to store, process and transport information assets
- SharePoint, file transfer systems, removal media, HR systems and financial system

As IAO the identification and management of the highest risk assets is key and knowing when to apply additional security controls to protect them.

Threat	Source or cause of risk - What can go wrong
Risk	Impacts/consequences/effects that an event can have on an organisation
Risk assessment	Overall process of risk identification, analysis & evaluation
Risk Management	Coordinated activities to direct and control risk

When assessing information risk, consider consequences if those risks were realised, including:

- Financial - Direct loss of revenue to the organisation
- National economic impact GDP
- Societal - Welfare and economy
- Reputational damage - National strategic partners/general public perception
- Process corruption - Democratic process, policy and strategic decision-making
- Legal/Law enforcement and criminal prosecutions/GDPR
- Physical harm - To persons identified due to compromise or unauthorised disclosure
- Operational - access to systems and assets that disrupt the ability:
    - to deliver organisational essential services
    - to deliver essential services to the UK population
- Loss, theft, leaking, unauthorised disclosure, or deletion of the information
- If the information could be used to harm UK interests or individuals
- What are the implications of failing to preserve the confidentiality, integrity, or availability of the information?

Framework for managing risk

The Framework for Managing Risk in HM Government outlines several common methods and tools however you should follow the processes used in your organisation.

IAOs should familiarise themselves with the risk-management practices within your organisation 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 risk-based decisions you make regarding assets for which you are responsible, within the wider organisation approach.

The most critical aspect of any risk assessment is implementing measures to ensure risks are mitigated to an acceptable level. The outcome of your risk assessment should identify the most sensitive information and the riskiest activities in terms of information handled across the organisation.

What are the threats and risks to information?

Your organisation relies on systems and technologies to handle information which is accessed by staff, partners and suppliers from diverse environments, including at home, the office, hybrid working or working overseas.

Threats to information could include a lack of appropriate measures to protect information, or from people seeking to take advantage of those vulnerabilities.

Threats to government organisations' information assets include:

- **Cyber criminals** – Ransomware is becoming increasingly widespread. Cyber Criminals are utilising malware to incapacitate organisations for money
- **State Actors** - may try to access technology or information for an advantage
- **Investigative journalists/the media** - are interested in a story about government – often publishing that information is not being handled well
- **Organised Crime** – criminal activity including theft and fraud
- **Terrorism** - remains a consideration, for any Government department
- **Single issue activists** – often driven by ideology, or desire for political influence
- **Man-made disasters** - terrorists, protest groups

Methods of attack may include:

- **Phishing and Social Engineering**: techniques involve tricking individuals into revealing sensitive information or performing actions that compromise security

- **Cyberattack:** malicious software, such as viruses, worms, and trojan horses, which can disrupt systems, steal data, or grant unauthorised access

- **Supply Chain**: vulnerabilities in third-party systems or vendors can lead to breaches in HMG's own networks

- **Data Breaches** - accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information potentially leading to loss of confidentiality, integrity, or availability of information

- **Cybercrime** - criminal activity carried out using the internet, including theft and fraud

- **Espionage** – Foreign state actors engaged in accessing UK sensitive information for geo-political or other nefarious motivations:

    - **State-sponsored espionage** – Targeting government or critical infrastructure for geopolitical advantage
    - **Industrial espionage** – Targeting commercial entities to gain competitive or economic advantage i.e. trade secrets, R&D and IP

- **Insiders** – employees, contractors or business partners, who intentionally or unintentionally misuse their legitimate access which can manifest in data breaches, data loss, or compromising critical systems

- **Man-made disasters** – terrorists, protest groups

How to understand the value of information to your organisation

Understanding the value of information assets helps to assess risks and opportunities. An information asset has an identifiable and manageable value to the organisation.

Organisations may have different risk appetites for high and low-value assets. Risk appetite refers to the amount and type of risk that an organisation is willing to accept to achieve strategic goals.

Government Digital Service

Government Skills

As an IAO, you can monitor risks more effectively by prioritising assets based on their value. Ensure assets within your area of responsibility are not overprotected or under-protected.

These questions will help you understand the value & sensitivity of your assets:

- Is it a business-critical or sensitive asset?
- What is the classification?
- Does the asset contain personal data and does any personal data fall into special categories?
- Could your organisation function without the asset for hours/days/weeks?
- Who can access the asset and who is it shared with?
- If the asset is combined with another piece of information does that increase its sensitivity (aggregation)?
- Does the content relate to your organisations business objectives?
- Is the information already published?
- Is the asset shared or created by your organisation, or by a partner?
- Would there be impact on operational efficiency if it wasn't accessible?
- What organisational objectives and processes does it support?
- Would loss or inappropriate access cause reputational damage to your organisation?
- Would it cost to replace or repurchase the information?

Government Digital Service

Government Skills

Scenario 3

Conducting an annual review of an Information Asset will support an Information Asset Owner's understanding of responsibilities during key moments in the information asset lifecycle.

Maria is an IAO accountable for an asset of datasets containing sensitive personal information collected through a housing support programme. The datasets include names, addresses, income details, and support needs of applicants.

Annual Review Process:

1. **Preparation -** Maria receives a reminder that the annual review of her asset is due. She asks the information asset manager to review the asset and update it with any changes

2. **Review -** Once the asset has been updated, Maria reviews the asset to confirm that she considers the asset record to be accurate. Some of the things Maria notes include:
   - Artificial Intelligence is now used to process some information contained in the asset which has not been noted in the asset record
   - A new risk has been raised in relation to an information-sharing partner

3. **Sign-off -** Maria requests the asset to be updated with the missing information before signing it off
   - Maria follows her department's risk management procedures to ensure that the risk in relation to the sharing partner is managed appropriately

The asset is updated and signed off within the department's information asset management policy timescale. Maria feels sufficiently informed to be able to make decisions about the management of the asset.

Key Learning Points

In this chapter, you explored the basics of information risk management.

Asset identification is the foundation on which all risk management is built.

The goal is to reduce the chances of a successful attack or mitigate its impact by applying appropriate security measures.

You are now aware of common risks to your information assets and threats to government organisations, including attack methods.

You learn to value information, identify critical assets and understand risk impacts, enabling prioritisation of controls to prevent breaches and avoid legal, financial, reputational and other damages.

Government
Digital Service

Government
Skills

Please check with your own organisation for further guidance on its information, risk management policy, process and procedure.

You have completed this chapter

Please start chapter 8

Government Digital Service

Government Skills

Chapter 8. Security Incidents & Data breaches

As an IAO being able to identify and understand specific actions, weaknesses in control or potential vulnerabilities and threats that may lead to an incident or breach, allows you to apply measures to mitigate against.

However, learning from past incidents can strengthen governance, promote a security culture, and improve risk management practices.

What are security incidents & breaches?

You should be informed of all incidents, especially involving information compromise for information assets within your area of responsibility. Data breaches that risk individuals' rights and freedoms must be reported to the ICO within 72 hours. GDPR compliance requires preparation and mitigation measures for such breaches.

A security incident involves the attempted or actual unauthorised access, use, disclosure, modification, loss, or destruction of an asset in violation of security policy.

A breach of security is defined as an incident where the procedures for managing the organisation's information or equipment have been violated or ignored.

What is a personal data breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information transmitted, stored or otherwise processed, according to the Information Commissioner's Office (ICO).

Government Digital Service

Government Skills

Examples of types of information & cyber breaches

(this list is not exhaustive)

Information Breaches:

- **External Disclosure:** Sensitive information is shared with or exposed to unauthorised individuals outside the organisation intentionally, unintentionally or maliciously.
- **In Transit:** Sensitive information in physical documentation is disclosed during transfer from one location to another.
- **Internal Disclosure:** One or more persons employed by or contracted to the organisation receives, sees or hears sensitive information with no legitimate reason to do so.
- **Redaction:** Sensitive information that should have been removed remains accessible to those unauthorised to view or is held on an unauthorised platform. This can involve personally identifiable information (PII), financial details or sensitive business data.
- **Verbal:** Sensitive information is shared verbally via conversations, phone calls, meetings, or any situation where confidential information is discussed in an unsecure environment.
- **Waste:** Physical documents containing sensitive information are not correctly or securely disposed of. This can expose data to unauthorised individuals, leading to potential misuse or unauthorised access.
- **Written:** Sensitive information is shared through handwritten or printed documents such as notes, letters, reports, or any written material not properly secured that falls into unauthorised hands.

Cyber Breaches

- **Cyber Access Rights:** Unauthorised individuals gain access to systems/network/data. By exploiting vulnerabilities, using stolen credentials or abusing granted access rights.
- **Data Transfer Security Issue**: Sensitive data is transmitted over network channels without encryption or security measures. Can lead to interception, unauthorised access or modification.
- **Social Engineering/ Malicious Software Phishing/Spear phishing/Whaling:** A targeted system or device, attacks staff with fraudulent emails, to deceive recipients into clicking on malicious links. Use of malware, viruses, worms, trojans, ransomware etc.

- **Leak:** The unauthorised disclosure of sensitive, confidential, or protected information, either intentionally or accidentally. This can be a deliberate leak of sensitive information to the press.
- **Social Media:** Sensitive, information is shared or leaked via social media platforms. Posting sensitive details e.g. on WhatsApp or in private messages between colleagues using social media.
- **External Misuse:** Unauthorised individuals outside the organisation such as hackers or cybercriminals either attempt to access or gain access to systems.
- **Internal Misuse and Breach:** Unauthorised individuals within the organisation abuse access rights to data/ systems. This could involve accessing sensitive information without authorisation, altering data for personal gain or leaking sensitive information.

Examples of real-world breaches and incidents

Security incidents affect an organisation's assets, potentially resulting in significant consequences. These real-world examples which occurred in the public sector illustrates how breaches can happen when security policies are not followed, and the consequences can be damaging to individuals and the organisation.

Breach 1. Physical Security Breach - sensitive waste

In February 2022, a government organisation experienced a security breach when 14 bags containing sensitive documents was left unsecured for 18 days, after a scheduled shredding service missed the collection. The bags included staff and other individuals medical and vetting information.

The bags, some unsealed were left accessible to both staff and unauthorised individuals. Although some staff challenged individuals seen handling documents, the incident was not reported to security. This breach exposed sensitive and personal information.

This lapse in security protocols could have led to significant distress, exposing staff and other individuals to the risk of identification and potential intimidation, including their family members.

Breach 2. Personal Data breach

A UK police force faced a major data breach when an employee, responding to a freedom of information request, inadvertently included a hidden worksheet with sensitive data in a workbook. This mistake exposed the personal details of over 9,000 employees online, including surnames, initials, rank, and role. This breach caused serious safety concerns for the individuals and their families.

Upon reporting the breach to the ICO, the event was described as a 'perfect storm of risk and harm,' emphasizing the human impact of inadequate data security. The police force was fined £750,000, reduced from £5.6 million due to public sector considerations. The ICO stated that this incident serves as a reminder for all organisations that simple procedures could have prevented the breach.

Potential impact and consequences of breaches

An information loss can cause harm or distress to individuals and have an impact on the organisation. Here are some examples of the potential consequences of breaches:

- **Personnel Risk**: Data breaches can expose sensitive personal information that could be exploited for identity theft and fraud. In some cases, can be life threatening
- **Regulatory Consequences**: The ICO often launches investigations, and the organisation can face penalties under the UK GDPR
- **Reputational Damage:** Public and parliamentary scrutiny over cybersecurity practices. Trust in Government is broken
- **Operational Disruption**: Internal reviews and audits / temporary suspension of certain digital services, affecting workflow and morale
- **Legal/financial:** damage to the organisation

How to avoid incidents and breaches

These incidents could have been avoided. So, what action can you take to prevent these types of security breaches?

1. Ensure staff within your area of responsibility understand the process for disposal of sensitive information securely and follow your organisation's procedures for secure shredding of waste or secure disposal. If sensitive information is left unattended it should be stored away securely and reported immediately to security.
2. Ensure staff within your area of responsibility understand they must never share official information on unauthorised platforms or systems. If information is shared accidentally on an insecure platform, the incident should be reported immediately to security.
3. Ensure staff within your area of responsibility handle information securely based on its classification and the 'need to know' principle and apply vigilance to always report potential breaches to security as soon as they become aware of them.

Sharing information safely – some actions staff can take to ensure they are sharing information safely include:

- Check for hidden data in attachments
- Check the recipients are correct and that they are authorised to receive the information
- When emailing multiple recipients, use bulk email services, mail merge, or secure data transfer services where available
- Always check sending emails to the correct recipient and be extremely careful when using the blind copy function (BCC)
- Do not use the BCC copy when sending sensitive information to multiple recipients via email. Consider sending individual emails instead

For further information regarding how staff can share securely visit the Share with Care webpage.

Reporting incidents and breaches

Staff should understand their responsibilities and what they need to do in their department to report a potential incident or breach. Any breaches involving personal information must also be reported to the data protection team.

Managing incidents and breaches

An organisation needs a well-established Incident Response Plan to manage breaches and security incidents effectively, aiming to prevent further damage.

Each organisation follows its own process for breach-reporting and investigation between the Data Protection Officer (DPO), cyber, and security teams. Many breaches may involve personal data, cyber elements, or physical components, adding complexity to their nature.

Therefore, it is essential for an IAO to ensure collaboration between these teams, especially during incident investigations, to gain a comprehensive understanding of the breach's cause and implement measures to mitigate future incidents. Effective incident response requires cooperation between the teams, with clearly defined roles and responsibilities to handle incidents and learn from them for future prevention.

Government Digital Service

Government Skills

Scenario 4

An IAO needs to understand the importance of knowing whether information is being handled and shared securely in the organisation.

A government department was asked to share data with an external party.

- The requested information included full name, staff number, job title and work email address
- The information was downloaded as an Excel file, within a single worksheet, from the department's human resources management system. This contained more information than originally requested, including full name, staff number, job title, salary details, health/wellbeing & disability information, criminal convictions & criminal offence data
- As the information was analysed before disclosure, multiple other worksheets were created within the downloaded Excel file
- On completion, all visible onscreen worksheet tabs were deleted from the Excel file, however, the original worksheet, containing the personal details (including special category data and criminal offence data) remained unnoticed
- The document was shared with the external party as an Excel workbook

The government department were quickly notified of the incident by the external party. Having experienced a data breach in the past themselves, they had installed an integrated bespoke software programme which identified the hidden cached data contained in the Excel file.

The data breach would not have occurred if the government department had followed internal guidance & shared the Excel document as a 'clean' version (e.g. as .csv file, PDF or had used Document Inspector).

The scenario demonstrates how important it is for Information Asset Owners/Information Asset Managers to know how their information is being used. Had they ensured that each member of their team understood the risks involved in sharing data, & how to protect & manage information, the risk of a data breach would have been reduced.

Government Digital Service

Government Skills

Key Learning Points

In this chapter, you learnt about various types of security incidents and data breaches that can have significant impacts on an organisation and the people involved.

As an IAO, you learn that you can help prevent incidents and data breaches by implementing comprehensive security measures and by ensuring staff within your area of responsibility are trained to recognise and report security incidents immediately.

A tested incident response plan enables quick breach management to reduce damage.

Collaboration with security, cyber and data protection teams with clear roles and responsibilities helps to effectively manage incidents.

Learning from past incidents is key to strengthening security governance and putting measures in place to prevent further breaches.

You have completed this chapter

Please start chapter 9

Government Digital Service

Government Skills

Chapter 9. Leading and fostering a culture that values, protects and uses information ethically

An Information Asset Owner (IAO) must stay informed about the strategic landscape, to understand the importance and role of information governance and security best practices. This ensures that IAO leadership is effective.

The IAO role is crucial and requires support and expertise from other subject matter experts (SMEs) and multifunctional teams, to assist in assuring information assets and implementation of core responsibilities. By ensuring that the right processes are in place for effective risk management, data protection, information governance, security and ensuring all those involved have a clear understanding of their responsibilities, the IAO can lead and foster a strong culture that values, protects and uses information ethically.

To develop a good information management culture, the IAO can help by:

- Supporting the organisation to comply with information rights legislation
- Reiterating the need for staff handling their assets to complete the relevant training for their organisation
- Highlighting the value of their role and how they can help within their area of responsibility
- Ensuring staff understand their responsibilities when it comes to information security and use
- Encouraging senior leaders to consider and manage risks to information assets in their business areas
- Promoting the ethical use of information
- Establishing and maintaining communications within business teams about good information management practices to ensure it is embedded in business processes

Government Digital Service

Government Skills

Key Learning Points

Leading and fostering a culture that values, protects and uses information ethically means an IAO must lead by example to drive change.

IAOs must be the champion to ensure the organisation has systems in place to:

- Know what information the asset holds
- Know what enters and leaves it and why
- Know who has access and monitor their use
- Understand and address risks to the asset and provide assurance to the risk owner
- Ensure ethical use of the information, including responding to access requests

It is essential for these principles to be part of daily operations so that information security and assurance issues can be openly identified and discussed. An IAOs leadership following these principles helps build trust within the organisation, with external stakeholders and with citizens.

You have completed this chapter

Please start chapter 10

Government Digital Service

Government Skills

Chapter 10. Information Governance

Overview

An Information Asset Owner (IAO) will usually work to the Accounting Officer, who would often be the Permanent Secretary or Chief Executive of the department/ organisation and will work closely with the Departmental Records Officer (DRO), the Senior Information Risk Owner (SIRO), the Data Protection Officer (DPO) and Data Owners to ensure that duties are properly coordinated and assurances are provided to the relevant internal information governance boards (or equivalent).

The specific mechanisms of how these relationships operate will be up to the individual organisation as not all departments will have all of the roles mentioned and, in some cases, the same person may be carrying out the responsibilities of more than one named role.

Roles and responsibilities

The Accounting Officer has overall responsibility for ensuring that the information risks are assessed and mitigated to an acceptable level.

Data Protection Officers (DPO) assist organisations to monitor internal compliance, inform and advise on their data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner's Office (ICO).

The senior person accountable for information security risk, (sometimes called the SIRO) plays the main role in the management and protection of the organisation's information assets, with a particular responsibility for information risk.

Departmental Record Officers (DRO) lead on compliance with the Public Records Act and play an important role in the management of information within government departments.

Data Owners are senior individuals who are the dedicated owner of a logical grouping of data and have in-depth insights into the overall business strategy in their data remit.

Information Asset Manager (IAM) is a delegated role working on behalf of the IAO, with regular responsibility for the proper management of information in their business area.

An IAO will also work closely with, and seek advice from, their knowledge and information management teams, digital and data teams, cyber and security teams and data protection teams.

Scenario 5

In the event of a member of staff reporting a security incident, it is important to understand the roles and responsibilities of the teams available to support you.

Context:
David is an IAO for an asset which includes internal staff performance reviews, which are held in a third-party system. One morning, a member of his team alerts him to a potential data breach involving his asset.

Incident Response

1. Immediate Actions:

- David asks his team to establish the potential consequences of the breach and carry out any actions advised by the information security team to mitigate the incident
- He issues communication to staff in his team about the need to address the incident as a priority and that support is available for affected staff, including speaking to him personally

2. Investigation:

- David is provided with regular reports on how the investigation is progressing. He is informed that a security weakness has been identified which could result in further unauthorised disclosures. He makes the decision to temporarily suspend use of the software

3. Risk Assessment and Notification:

- The Data Protection Officer determines that the breach meets the threshold for reporting to the Information Commissioner's Office (ICO). David reviews and signs off on the ICO notification that has been prepared

4. Post-Incident Review:

- David is presented with a lessons-learnt report. He decides to take forward all recommendations, except for one which would result in a disproportionate restriction on staff carrying out their roles, raising the likelihood of other risks materialising
- He updates the department's risk register and initiates a review of similar assets to prevent reoccurrence

Outcome:
The breach is contained quickly, and no evidence of misuse is found. David was given the information he needed to make reasoned decisions about how to handle the incident without the need for technical expertise or in-depth knowledge of the processes involved. The risks associated with this asset are managed more effectively and reoccurrence of a similar incident is less likely.

This scenario demonstrates the importance of recognising the roles and responsibilities of other teams and utilising them to achieve common goals, including addressing security incidents and data breaches.

Information Governance

The IAO has a vital role in connecting multidisciplinary teams to enable the exploitation of information within their area of responsibility, whilst complying with legal, regulatory and policy requirements.

The development of a culture that values, protects and uses information ethically is essential to ensuring maximum benefits are realised from the IAO role.

With the rapid development of AI systems and services, IAOs will become increasingly important in enabling the ethical, safe and explainable use of government information in those systems.

You have completed this chapter

Please continue to the knowledge checker

Government Digital Service

Government Skills

Module: Knowledge Checker

Welcome to this assessment of the IAO course. You should attempt the questions after completing the course chapters 1 – 10.

There are 10 short questions. You will need to answer 8 correctly out of 10, for 80% score to pass.

Keep your own record of your answers. You can find the correct answers for each question at the end of the Knowledge Checker.

Please allow 5-10 minutes for completion.

1. What is the definition of an Information Asset?

a. An IT system or application used by your business area

b. Documentation that includes personal data

c. A body of information, defined and managed as a single unit

d. A set of documents stored in a SharePoint library or Microsoft Teams site

2. An IAO can delegate accountability to a member of their team?

a. True

b. False

3. Which of the following group form part of the Government Security Classifications?

a. OFFICIAL, SECRET, TOP SECRET

b. OFFICIAL-SENSITIVE, RESTRICTED, SECRET

c. OFFICIAL, SECRET, TOP DATA

Government Digital Service

Government Skills

4. To comply with GDPR law, what process should be undertaken for all new projects or changes to processes to identify potential risks to personal data?

a. Data Transfer Assistance (DTA)

b. Data Protection Impact Assessment (DPIA)

c. Data Development Initiative (DDI)

5. What formal process or system can be used to provide an IAO with oversight of the information assets held across the entire organisation?

a. Information Action Sheet (IAS)

b. Information Asset Register (IAR)

c. Information Asset Holder (IAH)

6. What are the potential consequences of a data breach?

a. Cause harm to an individual whose data is involved in the breach

b. Cause disruption to risk management

c. Provides the organisation with strategic information

7. What is the most critical aspect of any risk assessment?

a. Implementing measures to ensure risks are mitigated to an acceptable level

b. Checking there are risks present and are fine

c. Creating a process that looks at what impact has been realised

8. Which statement represent the purpose of risk assessments?

a. A risk assessment assesses the effectiveness of staff measures to protect assets

b. A risk assessment considers policies, regulatory constraints and business objectives.

c. A risk assessment should identify the most sensitive assets and riskiest activities in terms of information handled across the organisation.

d. All of them are correct and apply

Government Digital Service

Government Skills

9. When should staff be encouraged to report any incidents and breaches?

a. Immediately when they suspect a breach or incident has occurred

b. Only if they are involved or were responsible for the breach

c. Only if they are 100% certain and can evidence a breach has occurred

10. Which teams or experts should an IAO engage and collaborate with to ensure good information governance and security of information in the organisation?

a. Knowledge and Information Management

b. Digital and Data, Cyber Team, Data Protection Officer

c. Security & Assurance

d. All the teams listed

Answers

1. C
2. B
3. A
4. B
5. B
6. A
7. A
8. D
9. A
10. D

Government Digital Service

Government Skills

This training was developed in collaboration with our partners across government