Government
Digital Service

Government
Skills

Information Asset Owner

Core Activities

Government Digital Service

Government Skills

The Information Asset Owner (IAO) role comes with responsibilities in support of a culture of best practice. This includes core activities for the 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 IAOs, working with their Information Asset Manager and teams:

- **Accountability:** Maintaining clear accountability 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:** Of all information assets within the domain. Determining what constitutes an information asset and categorising it based on its importance, sensitivity and usage

- **Valuation:** Assessing the value of the organisation's information. Identification of the highest value assets and applying appropriate additional security controls. This helps in prioritising resources to the most critical assets

- **Risk Management:** Identifying and mitigating risks associated with information assets. This involves evaluating current risks, implementing mitigation measures and monitoring emerging risks. Ensure assets are managed in line with the organisation's information risk appetite

- **Security:** Implementing and overseeing 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:** Maintaining an accurate and up-to-date Information Asset Register. This includes documenting details such as the asset's location, the owner, the classification and including any new assets or changes in status

- **Data Usage & Access:** Monitoring the usage, make decisions on use, transfer, and access controls. Where needed, have data sharing agreements and memorandums of understanding 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 helps in sharing insights and aligning efforts and resources

- **Compliance:** Review and ensure management and usage of information assets, comply with the relevant regulations, policies and standards, and adjustments are made 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:** Engaging 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:** Overseeing 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 seeking ways to improve the management and protection of information assets. This involves staying up to date with best practices, technologies, and regulatory changes

- **AI:** 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)

- **Information Governance:** The IAO has a vital role in connecting multidisciplinary teams to enable the exploitation of information within their area of responsibility, while complying with relevant legal, regulatory and policy requirements. The IAO also develops a culture that values, protects and uses information ethically

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 to 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).