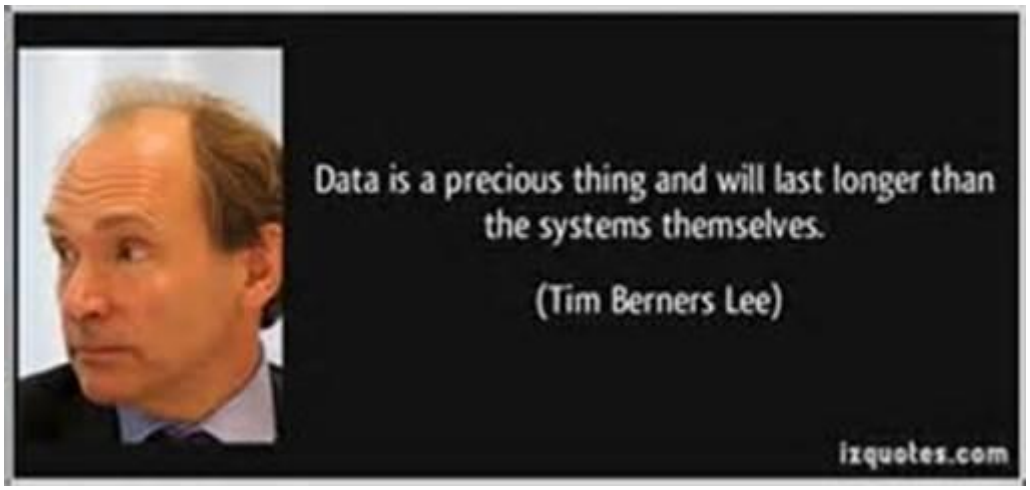
Information Asset Owner's Handbook



Index

	Page Number
Introduction	**3**
Reporting chain	**3**
Who should hold the role of Information Asset Owner?	**3**
Definition of an Information Asset	**4**
How to identify an Information Asset	**4**
Information Asset Register	**4**
Removing assets from the IAR	**5**
Risk Management	**5**
Definition of Information Risk Management:	**5**
Risk Assessment	**6**
Potential risks to your assets	**6**
Risk Management	**8**
Risk Assessment & Reporting	**8**
Annual judgement for Governance Statement	**8**
Information Assurance culture/behaviours	**8**

Introduction

The Security Policy Framework sets out how HMG must handle its information to ensure its sensitive assets are robustly protected. The Framework states organisations should appoint and train Information Asset Owners (IAO) for each of their information assets. An IAO reports to the Senior Information Risk Owner (SIRO) and their role is to protect and manage information held in HMG and ensure its value to the organisation is fully exploited.

This handbook will help you to understand your role and responsibilities as an IAO within Highways England; the chain of governance (including where you fit in) and the skills you need to be effective within the role.

Reporting chain:

Accounting Officer (Chief Executive): Has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level.

SIRO: Responsible for ensuring that information risks are managed appropriately – Vanessa Howlison is the SIRO for Highways England.

IAO: Responsible for day-to-day management of information risk for their asset.

Who should hold the role of Information Asset Owner?

IAOs are senior/responsible individuals working in a relevant business area. Their role is to understand what information is held, what is added and what is removed, how information is moved, who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good. When identifying an IAO, consider the risk to the information asset rather than the size of the asset. The IAO need not be the creator, or even the primary user of the asset, but they must have a good understanding of what the business needs from the asset and how it is used.

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

- Identifying risks associated with the information asset;
    - Understand and address risks to your information assets
    - Understand whether a delivery partner or supplier has a dependency on your information to deliver a service and how they use and protect that information
    - Make sure your information assets are fully used for the public good, including responding to access requests and alignment with the Transparency Agenda
- Managing and operating the asset in compliance with policies and standards;
    - Be aware of and understand relevant statutory requirements with regard to handling information
    - Check that access provided is the minimum necessary to achieve the business purpose

    - Consider requests for access to information from other business users, and maintain log of requests and decisions
    - Report breaches promptly in accordance with the company's breach reporting process
- Ensuring controls manage all risks appropriately.

Definition of an Information Asset

An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. An asset can be a single significant document or a set of related data, documents or files; it can be shared or be confined to a specified purpose or organisational unit.

How to identify an Information Asset

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

- Does it have a value to the organisation?
- Will it cost money to reacquire the information?
- Would there be legal, reputational or financial repercussions if you couldn't produce the information on request?
- Would it have an effect on operational efficiency if you could not access the information easily?
- Would there be consequences of not having this information?

Further information regarding how to identify an information asset can be found here: Defining and identifying Highways England Information Assets

Information Asset Register

The Information Asset Register (IAR) lists the company's information assets alongside their associated owners (IAOs). The IAR is a list of personal and business critical information assets. Examples of the type of information held on an IAR are:

- Description and purpose of asset
- IAO details
- Risk assessment (Confidentiality, Integrity, Availability)
- If the information is held/processed by a contractor

It is essential that the IAR is up to date and accurately reflects the company's information assets. As an IAO, it is important you understand the company's processes for recording changes relating to information assets.

This can include:

- Assets being assigned to new IAOs
- Information assets no longer in existence
- New assets identified and included on the register

Removing assets from the IAR

An information asset may be superseded by other work, or have come to the end of its lifecycle. In such cases the IAO will need to determine whether the information asset still needs to be kept and if so, may want the IAR updated to highlight that the Information Asset carries a lower level risk than before.

Alternatively, it could be removed from the IAR as there is no longer a business need for it or it has been destroyed. IAOs need to ensure they gain the appropriate authority before any assets are removed.

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

Risk Management

IAOs should familiarise themselves with risk management practices, specifically how to identify, understand, manage, report and record risks. Understanding the company's risk appetite is also important, as it will help you to align any risk-based decisions you make regarding assets for which you are responsible with the wider organisational approach. Risk appetite can be defined as; the threshold relating to the level of risk the company acceptable and which should not be exceeded, unless approved by the SIRO.

An IAO's role is a key element in the company's efforts to manage information risk. The SIRO looks to IAOs for the day to day management of information risk and to highlight systematic risks which the company may need to address.

Definition of Information Risk Management:

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

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

- risk assessment;
- cost benefit analysis; and
- the selection, implementation, testing and security evaluation of controls.

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

Risk Assessment

Risk = Threat x Vulnerability x Likelihood x Impact

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

Threat – what can go wrong?
Risk – what is the chance of it happening?
Risk Assessment – what would be the consequences/impact?
Risk Management – what can be done about it?

Potential risks to your assets

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

Risk category	Example of risk	Example of threat
Governance and culture	Lack of effective governance arrangements, comprehensive oversight and control Lack of proper procedures for handling incidents, including identifying and acting on lessons learned Third parties letting you down (suppliers do not apply the same standards of information security as we apply ourselves)	New business services not taking risk information into account Culture that does not recognise the importance of protecting information at the same time as looking for opportunities to share and exploit it.
Information management and information integrity	Critical information is wrongly destroyed, not kept or cannot be found when needed Information becomes unreadable due to technical obsolescence Information is lost	Lack of basic records management disciplines or non-compliance with agreed processes. Inaccurate information Staff not following security policy or guidance with information in their care.

The human dimension	Despite having procedures and rules, staff, acting in error, do the wrong thing Inappropriate disclosure of information	Despite having procedures and rules, staff do the wrong thing deliberately (insider threat) External parties source your information illegally Staff not following guidance in relation to the asset
Information availability and use	Failure to disclose critical information for case management or protection Failure to utilise the value of the information asset Failure to allow information to get to the right people at the right times.	Staff not following guidance in relation to the asset ICT failure (availability)
Technology & cyber (IT systems)	Denial of service due to systems failure Corruption of data leading to delay in services	Denial of service due to an attack Spear Phishing Espionage or crime campaign Data leaves the service in an uncontrolled manner
Process disruption	Established processes disrupted by new regulation or government guidance Focus on compliance with security processes and procedures at the expense of business performance	

Information risks are threats to:

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

Risk Management

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

- What organisational objectives and processes does it support?
- What is the asset there for? What would happen if you couldn't use the system or access the information on it?
- What are the outputs and outcomes that would be affected if there was a problem?

Risk Assessment & Reporting

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

Annual judgement for Governance Statement

The annual statement of assurance confirms that internal controls are being managed within the company and that issues identified are being addressed. Information Asset Owners have a responsibility to understand what information is held, in what form, how it is added and removed, who has access and why. As IAOs you need to understand, identify and control risks to the business in relation to your asset(s) and provide annual assurance to the SIRO.

Information Assurance culture/behaviours

IAOs are not only responsible for identifying, understanding, managing, reporting and recording risks in relation to their information assets, you also have a role in leading and fostering a culture that values, protects and uses information for the benefit of both the public and the company. IAOs need to champion good information handling and support information assurance culture change activities. IAOs have a particular responsibility to ensure they maintain an awareness of any policies or guidance in relation to Information Management (IM) and also ensure these are followed by those who have access to their information assets, which may include third parties such as the supply chain.

The Information Assurance cultural vision is: *"to foster an organisational culture*

that values, protects and uses information for the public good"

The high-level culture change outcomes are:

- Leaders recognise the importance of good information management and champion cultural change activities
- Everyone is aware of their responsibilities with regard to the management of information and behaves appropriately
- Everyone has the appropriate skills needed to manage information effectively within their role
- Staff in specific mandated roles have clear terms of reference
- Good information management is recognised and rewarded appropriately
- Appropriate action is taken in cases of breaches or non-compliance

This vision is reflected within the HE Co-ordinated Data Improvement Plan (CDIP). CDIP highlights the increasing expectations on our Board to assure the quality of reporting and the internal decisions to support our investment programme which link directly to the quality of our underlying data.

HE operates in a regulated environment in which the Highways Monitor, the Office for Rail and Road (ORR) can request any reasonable information and data at any time. As a public company we are also open to public scrutiny and are subject to a number of key pieces of legislation, including the Freedom of Information Act, the Data Protection Act and the Public Records Act. Data is therefore at the heart of everything we do and our culture needs to become one in which we treat data as a strategic asset.

Vanessa Howlison as the SIRO has responsibility not only for defining our corporate information risk appetite, but for overseeing all aspects of information risk and assurance. The role of the IAO within Highways England is to support the SIRO by assuring, developing and maintaining business critical data sets for operational and assurance purposes.

For further information on the Information Asset Register and the role of the IAO please contact the Information Compliance & Assurance Manager