The National Archives

Information Management Assessment

A review of good practice from the IMA programme, 2008-16

Section 3: Information risk and governance

Working with government to raise standards in information management

Contents

Note: references are to the named individuals, roles and organisations as they operated at the time of the Information Management Assessment or progress review

1. Recognising information risks

IMA Goal: The organisation defines and manages information risks to minimise threats and maximise opportunities.

Documenting and describing information risks

We have found that risks relating to the security of information are often better understood and more clearly defined than those relating to the management of information. However, the impact of a failure to capture, keep or dispose of information as required may be no less significant than that achieved through physical loss or a leak. Poor IT infrastructure, lack of governance and a non-compliant culture are all potential contributing factors.

The Section 46 Code of Practice highlights the importance of including information and records management within the corporate risk management framework.[1] Our assessments consider whether strategic risks are being monitored centrally and business areas are taking ownership of compliance at a local level.[2] Team, project and departmental risk registers should proportionately but clearly set out the effect of a failure to capture and keep information in line with corporate guidance; they should also define mitigating actions that will promote and enable good practice.

Ministry of Defence (MOD), 2014 progress review

If risks are not defined formally, they cannot be managed consistently. MOD identified information and records management as a key risk area within its 2014 Departmental Improvement Plan. In addition to this, MOD has clearly defined and captured information and records management related risk within its corporate risk management framework:

> 'MOD has worked pro-actively to define and formalise its understanding of information and records management related risk in a way that can

[1] nationalarchives.gov.uk/information-management/manage-information/planning/records-management-code/
[2] nationalarchives.gov.uk/information-management/manage-information/ima/

easily be reported at a senior level … [The] detailed Risk Assurance Matrix is an excellent model of how to capture risk and define actions arising. The Matrix breaks down information and records management related risk under headings such as leadership, policy and guidance, culture and skills and IT tools. It is updated regularly and presented quarterly to the Defence Board. Mitigating activity is plotted against each risk – for example, the need for training, updating policies or behavioural change – thus recognising the multi-faceted nature of both the risk and the ways of addressing it.'

Home Office, 2015 IMA

Home Office had identified a strategic-level risk relating to information exploitation. The IMA report noted:

> 'The Home Office is one of a small number of departments among those we have assessed to have done this. By defining this risk, it has demonstrated that it understands the value of the information that it works with and the potentially significant impact if this value it is not realised effectively.'

Beneath this level, on its Corporate Services risk register, Home Office had an effectively described information security risk from which it had separated out an information availability related risk owned by the DRO. We noted that the information availability risk Home Office had identified highlighted

> '… a range of cultural and IT-related causes. The risk description clearly establishes the impact of poor performance in information and records management for the department … Undergoing an Information Management Assessment has been included among mitigating actions in recognition of the benefit that can be obtained from external scrutiny and review.'

Ministry of Justice (MOJ), 2016 IMA reassessment

We saw good evidence that MOJ recognised the potential impact of information integrity and availability related risks. MOJ had defined the following IM related risk:

> **'RISK:** Information (electronic and paper) and records are not stored in correct locations and/or retained for correct lengths of time.
>
> **CAUSE:** Insufficient understanding by the Department of the value of good information management. Lack of an overall information management strategy. Managers and staff not fully aware of the need to correctly organise, make available and destroy/archive information. Current technology provision makes it difficult for staff to manage information well.
>
> **EFFECT:** Department cannot implement the governance to support the information principles. Reputational damage to the Department. Harm and/or distress to individuals, breach of information legislation. Adverse impact on compliance with Goddard Inquiry. Increased probability a technical compromise of systems will lead to a data breach.'

The IMA reassessment report noted that a range of appropriate mitigating actions were listed covering policy, guidance, training, disposal, and analysis of shared drives.

Department for Education (DfE), 2015 IMA reassessment

DfE required its staff to record information risks in business risk registers, with an escalation route through unit risk registers. We saw evidence that information and records management related risks were being defined in line with policy requirements. The IMA report noted that one local risk register included a risk relating to

> '… decisions, issues and evidence… not [being] sufficiently recorded, leading to potential reputational damage if decision reviewed by external body or committee.'

To mitigate the risk, the business area recognised the need to

> '… put in place strong Project and Programme Management measures, including risk management and assumptions logs. We will agree clear decision-making process with stakeholder groups to ensure all decisions and supporting evidence are captured, mapping decisions ahead of time, [and] adhere to good records management processes.'

Implementing an information risk management approach

The creation of an information risk policy is one of the mandatory minimum requirements for all government departments, introduced in support of the Security Policy Framework.[3] The policy should define how information risks will be managed and how the effectiveness of processes and controls will be assessed:

> 'In so doing the policy supports the organisation's strategic aims and objectives and should enable employees throughout the delivery chain to identify an acceptable level of risk, beyond which escalation of risk management decisions is always necessary. The policy fits within the organisation's overall business risk framework; information risk need not be managed separately from other business risks. [4]

We recommend that organisations use their information risk policy to codify the potential impact of poor performance in information and records management. Organisations should also set out the required standards that have to be met and establish the information and records management function's role within the overall risk management structure.

We assess the structures that are in place, how risks are owned, the plans that are in place to mitigate them and whether Senior Information Risk

[3] www.gov.uk/government/collections/government-security
[4] www.gov.uk/government/uploads/system/uploads/attachment_data/file/365968/Guidance_on_Departmental_Information_Risk_Policy_v1_1_Apr-13.pdf

Owners (SIROs) and departmental Boards are engaged and providing leadership.

Cabinet Office, 2013 IMA

Risk-related policy documents promoted a broad interpretation of information risk. Information and records management was specifically referenced and the potential impact of poor performance was established:

> 'The department's 2012 information security policy recognises the Public Records Act among the significant legal and regulatory requirements placed upon government departments. The policy also defines the role of the Head of KIM in ensuring records compliance. The separate information risk policy makes a strong statement that "poorly managed information can lead to a material impact on an organisation; financially, reputationally and even legally". The policy underlines the need to dispose appropriately of information and data when they are no longer required.'

Ministry of Justice (MOJ), 2016 IMA reassessment

We recognised that MOJ had put in place a framework that enabled the effective management of information risk through the department's SIRO Board and supporting Information Assurance Leads Committee. The IMA report noted:

> 'The SIRO Board reviews the MoJ Information Risk Register that covers significant information risks from across the Department ...
>
> 'The purpose of the SIRO Board is to ensure that MoJ 'achieves the required standards of information assurance and compliance' through agreeing strategies and policies, supporting and prioritising information risk management activities, and ensuring that there are adequate and joined-up governance structures. Through this board, information risks are visible to the [departmental] SIRO, and group SIROs who are senior business representatives.'

2. Establishing control

IMA Goal: The organisation has effective governance structures in place that foster communication and strategic planning.

Service delivery and governance structures

Organisations should put in place a proportionate governance framework for information and records management that includes defined roles and lines of responsibility. The IMA programme lessons learned report states:

> 'Good information and records management governance and culture will enhance the success of KIM strategies and policies in practice.'[5]

We consider whether KIM functions are planning effectively and working to deliver a defined service to the business. A key consideration is what governance boards and structures are in place to support communication and collaboration between KIM, IT and information assurance functions.

Home Office, 2015 IMA

The newly-created Knowledge and Information Executive Group (KIEG) was being set up at the time of the IMA. It was due to be chaired by the DRO and to meet on a quarterly basis. Following the IMA, links were established between the KIEG and the department's Data Board. The DRO became a member of the Data Board and the Head of KIM Direction joined the Board sub group. The IMA report noted:

> 'The KIEG will be attended by Senior Civil Service-level representatives from the Home Office Directorates and Arms' Length Bodies. These staff will assume the newly-created role of Knowledge and Information Champions, and may be represented at meetings by a deputy at a level no lower than Grade-7. The board will also be attended by subject matter experts from Home Office Technology, Corporate Security and

[5] nationalarchives.gov.uk/information-management/manage-information/ima/ima-reports-action-plans/

the Office of the Chief Digital Officer.

'The Board's senior membership and a defined escalation route up to Executive Management Board level have the potential to provide real impetus to the Home Office's efforts to improve performance. Its creation is likely to increase central oversight and improve understanding of local dynamics.'

HM Treasury, 2015 IMA reassessment

HM Treasury had recently established an Information Management (IM) Steering Group that met every two months. It was chaired by the DRO and Head of KIM. The IMA report noted:

'Membership includes the Chief Technology Officer (CTO) and representatives from Internal Communications, IT Services, Knowledge Management, Site Owners, IT security and technical specialists. It will:

- Develop and own a list of strategic IM priorities, which will help clarify where we are, where we'd like to be and how we get there.
- Review new requirements for IM services and technologies and advise the Change Board, who will ultimately respond to them.
- Consider conflicts amongst business teams for change resource in order to assist decision making by the Change Board.
- Advise IWS on which IM approaches will work best in Treasury and steer the direction of training and support services to fit.
- Advise on communications messages to help ensure that IM is well understood and received across HM Treasury.
- Adjust its governance principles where appropriate.'

The House administrations, The Houses of Parliament, 2016 IMA

Documentation established by the Houses administrations clearly set out the aims and objectives of the Information and Records Management Service (IRMS). This included a defined range of outreach activities:

> 'The Parliamentary Archives' Memorandum of Understanding and Statement of Services to be Delivered for 2015-16 establishes the basis for the shared service to be delivered in each financial year, setting out priority areas for IRMS and other archives staff, together with key staffing and governance requirements ...
>
> 'IRMS has produced a Customer Service Charter that was endorsed by the Business Management Group in the House of Commons and Business Planning Group in the House of Lords in July 2014. This sets expectations for the team in terms of service standards and for the business in relation to compliance with policy. The document identifies four main headings under which the team's work falls:
>
> - advice and consultancy
> - information risk assurance
> - building capacity
> - customer and system support.'
>
> 'The Customer Charter and these four areas were cross-referenced in the Memorandum of Understanding.'

Establishing support networks

As well as having a central information and records management function, organisations are likely to benefit from the use of centrally led networks to promote and champion good practice and support staff in the effective use of IT systems. These can be an effective means of regulating processes such as file creation and closure. They may also be utilised to monitor standards of information and records management, improve understanding of the challenges that staff face, and to challenge and address bad practice.

On-going effort is required to maintain networks and ensure staff remain engaged and are supported by managers to carry out their roles effectively. This should include reward and recognition. If a network has lapsed, it is important to recognise this and work to re-energise it.

Department for Transport (DfT), 2011 IMA progress review

Following its 2009 IMA, DfT reviewed the role of Business Record Officer (BRO), which had previously often been filled by junior staff. The department's progress review noted:

> 'The role of the BRO is being redefined to address the need for a more efficient, skilled and supported network. A specific BRO toolkit to support BROs and their managers has been produced.'

Department of Health, 2014 IMA

We found that the Department of Health was actively working to maintain and gain benefit from its centrally run network of Local Folder Managers (LFMs). The department produced a quarterly 'Why Information Matters' newsletter. The IMA report noted:

> 'The autumn 2014 edition gave the dates of forthcoming training sessions, IWS [the department's SharePoint system] news stories relating to forthcoming updates and improvements, requests for feedback, systems-related features and case studies. The department also holds regular sessions for LFMs, one of which the assessment team had the opportunity to attend. This was the third held in 2014, each session being offered at a number of dates, times and venues to help maximise attendance and participation. LFMs interviewed indicated that they found the sessions helpful and the assessment team found the session to be of good quality, offering an opportunity to promote priorities and quick wins and to address questions and concerns. Concerns raised by attendees included the lack of emphasis that some teams were placing on information management and difficulties leveraging change.'

HM Treasury, 2015 IMA reassessment

Two key support roles for information and records management had been established, based in business areas: Info Store Site Owners to help manage EDRM folders and Knowledge Champions to support KIM monitoring and improvement. Guidance stated that Knowledge Champions should be:

> '... an enthusiastic advocate of KM, who is able to coordinate KM activities and provide support for KM initiatives, monitor and report on the team's progress, and work with other Knowledge Champions and the Knowledge Manager to develop good practices.'

The IMA report noted that the Deputy Directors we interviewed recognised the importance of the Knowledge Champions, as their work helped business areas to achieve good results in HM Treasury's Knowledge Management Benchmarking process. Knowledge Champions helped facilitate this process, gathering evidence, facilitating meetings and developing action plans that were being used to drive improvements.

> 'The Knowledge Champions we spoke to were enthusiastic, proactive and took their responsibilities as Champions seriously. There are also monthly meetings for Knowledge Champions where they can discuss issues and share best practice.'

The House administrations, The Houses of Parliament, 2016 IMA

The information and records management team had a defined objective in place to develop the capability, awareness and skills of those holding the Record Officer role. The IMA report noted that, in addition to role-specific training, the team was providing a range of support, including

> '… an annual general meeting, a quarterly newsletter, targeted emails and an annual records officer desk calendar. The latter provides a helpful means of communicating key helpful information and reminders of key requirements for the role. The pages at the front of the calendar set out the main elements of the customer service charter and the "what to keep and where" guidance. The page for each month includes

a photograph from the Parliamentary Archives and a series of reminders on routine and date-sensitive activities that need to be undertaken. These range from setting retention trigger dates to reminding teams to review and clear out redundant emails. At the back of the calendar, there is an overview of how to unlock a document in SPIRE [the EDRMS], how to change a Record Officer password and the process to follow in relation to a change in Record Officer.'