

Information Management Assessment

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

Report summary

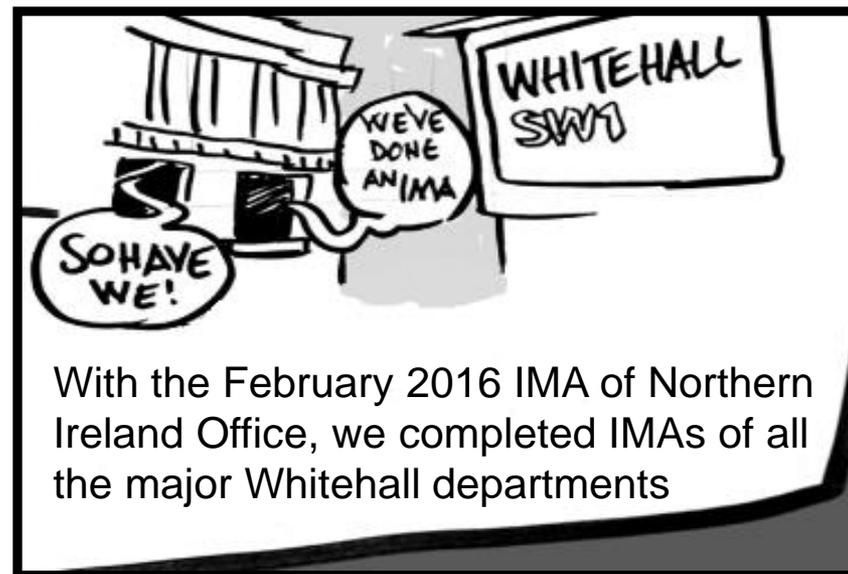


Working with government
to raise standards in
information management

The IMA programme is central to The National Archives' role as the government's expert in the management, use and re-use of information. Our current strategy is positioned to support *Archives Inspire*, The National Archives' business plan for 2015-19.

Participating in the IMA programme helps public sector bodies to

- assess their ability to meet legal and policy obligations
- meet the demands of increased volumes for transfer under the 20-year rule
- address the technical and intellectual challenges raised by the requirements to select, sensitivity review and transfer hybrid and digital records
- recognise the business benefits of protecting, managing and exploiting information effectively



With the February 2016 IMA of Northern Ireland Office, we completed IMAs of all the major Whitehall departments

The value of information

Communicating and realising value

IMA Goal: The organisation establishes information's value in principle and supports its realisation in practice

Telling staff why information management matters

Good information and records management doesn't happen by itself. IT systems can automate and simplify processes, but staff will still need to exercise judgement and invest an amount of time and effort to get things right.

The first step in helping staff do this is ensuring the value of information is understood.

Setting goals for information and its management

An endorsed and supported information strategy is a key means of driving increased capability.

We recommend a holistic, joined-up vision for the management, protection and exploitation of information.

Links between data, digital and technology, and information and records management goals should be defined.

The value of information

Communicating and realising value

Welsh Government 2014

A clear statement on the value of information was published prominently on the intranet: 'The knowledge and information we hold is one of our most important assets... Managing and protecting this information – particularly if it is sensitive or personal – is an important part of our role as civil servants.'

FCO 2014

FCO appointed their Chief Operating Officer (COO) as a Board-level champion. The COO supported the department's knowledge strategy, promoting the importance of good practice and sponsoring key communications.

Houses of Parliament 2016

Information management policy set clear expectations for managers, stating that they must both make sure that staff are aware of their responsibilities and that they are given sufficient time to carry out required tasks.

FCO 2014

Knowledge management was one of the 5 strands of the FCO IT strategy – the most effective example of a joined up approach we have yet found. The IT strategy set the clear aim of enabling better KIM through the introduction of an improved IT environment.

BIS 2013

The draft strategy set the aim: 'KIM is not an added task, it is how we work.'

The value of information

Managing, protecting and exploiting information assets

Information asset related guidance can be found on the digital continuity pages of The National Archives' website

IMA Goal: The organisation manages, protects and exploits its information assets to achieve maximum value

Defining and cataloguing information assets

Used effectively, the concept of an information asset provides a key means of enabling outcomes for the management and exploitation of information as well as its protection.

Key tools include Information Asset Registers (IARs): these should record context about information assets such as format, value and retention requirements.

Organisations should use the role of Information Asset Owners (IAO) to encourage good practice.

The value of information

Managing, protecting and exploiting information assets

UKEF 2015 [progress review]

The IAR had been expanded; it was no longer simply a list of IT systems.

UKEF now had a more detailed understanding of its information assets and asset clusters, which had been identified and catalogued following the IMA

DWP 2015

Information and records management was factored into information asset governance through

- Inclusion of retention on the IAR
- a question around compliance with the Records Management Policy on Information Asset Assurance Returns

The National Archives 2012 [progress review]

Information assets had been defined on the basis of disposal schedules; unstructured information was included as a matter of course.

IAOs were expected to report on steps taken to support transparency goals.

The Houses of Parliament 2016

Workshops run by the Information Ownership project encouraged teams to think about how information flows between them. The creation of IARs through the project had encouraged teams to rethink the sensitivity of their information assets and define new disposal schedules.

Information and supporting technology

NOTE: Many departments are moving to Office 365 with SharePoint or to a Google platform with Google Drive. We expect to begin assessing the success of this transition in 2017-18.

The technology environment

IMA Goal: The technology environment supports the management, protection and exploitation of information

The Section 46 Code of Practice states IT systems should be

- set up in a way that enables routine records management processes to take place
- easy to understand and use to reduce the effort required of those who create and use the records within them.

IT systems need to be maintained and developed and organisations should also restrict access to alternative storage locations that are not subject to oversight and control.

Information and supporting technology

The technology environment

NIO 2016

Take up of the EDRMS was better than in many other government departments. This was likely due to the fact NIO had eliminated or controlled alternative areas for storing information.

It was working to flatten its file plan to enable automated application of retention criteria.

Welsh Government 2016 [progress review]

Operations Group approved a project to

- identify how to improve the way staff use email and manage records
- tackle legacy storage in personal and shared spaces.

This helped drive a 64% increase in EDRMS usage.

HM Treasury 2015

A project was set up to address HM Treasury's digital legacy and redesign its SharePoint EDRMS to implement better policy compliance (by design) and enable digital preservation.

Requirements included mandatory requirements, records management requirements and business user input. They covered metadata, file plans, search, access permissions, retention and disposal, triggers for disposal and transfer to The National Archives.

Information and supporting technology

The continuity of digital information

IMA Goal: The organisation is taking proactive steps to ensure the continuity of its information, over time and through change

Encouraging joined-up planning

Organisations need to ensure that the digital continuity of their information is maintained over time and through change.

Organisations should also ensure that business requirements for information management are factored into system design from the start. Digital, data, technology and KIM staff should work together to build a shared understanding.

Digital continuity is about making sure that your information is complete, available and usable for your business needs. Your information is usable if you can

- find it when you need it
- open it as you need it
- work with it in the way you need it
- understand what it is and what it is about
- trust that it is what it says it is.

Information and supporting technology

The continuity of digital information

Department of Energy and Climate Change 2014 [progress review]

A tailored digital continuity strategy was created ahead of the move to the department's new records system: metadata and content could be maintained when information was migrated between systems.

HM Treasury 2015

IT and KIM functions were working closely together. The KIM team had the opportunity to feed in its view as a matter of course in relation to IT procurement and contracts

Ministry of Justice 2016

Digital continuity was being embedded into existing processes.

Risks around legacy systems and digital continuity are recognised as part of the MOJ risk management process.

IAOs are expected to conduct digital continuity risk assessments.

Information and supporting technology

Recognising information risk

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

Defining and managing information risks

Risks relating to the security of information are often better understood than those related to the management of information.

However, the impact of a failure to capture, keep or dispose of information can be just as significant as that of a physical loss or a leak.

Information management related risks need to be defined and recorded at appropriate levels within an organisation's risk management framework. Arrangements for managing this category of risk should be formalised in information risk policy.

Information and supporting technology

Recognising information risk

Home Office 2015

An information availability risk had been separated from an existing information security risk. It was owned by the DRO: it highlighted cultural and systems-related causes that could undermine effective information management.

MoJ 2016

MOJ recognised the risk of not storing information and records in the right place or for the right length of time.

A range of potential causes were identified. These included: a lack of recognition of the value of good information management; a lack of awareness of required process; and limitations of existing technology provision which makes it hard for staff to manage information well.

DfE 2015

Staff were expected to record information risks in business risk registers with an escalation route through unit risk registers.

A sample risk register included an information and records management risk. Mitigating actions included following good project and records management processes.

Cabinet Office 2013

Information security policy recognised the Public Records Act among the significant legal and regulatory requirements placed upon government departments. Information risk policy stated:

‘Poorly managed information can lead to a material impact on an organisation; financially, reputationally and even legally.’

Information risk and governance

Establishing control

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

Governance structures and boards

Organisations should put in place a proportionate governance framework for information and records management that includes defined roles and lines of responsibility.

Support roles

Organisations are likely to benefit from the use of centrally led networks to promote and champion good practice and support staff in effective use of IT systems.

However, ongoing effort is required to maintain networks and ensure staff remain engaged and supported by managers to carry out their roles effectively.

Information risk and governance

Establishing control

Home Office 2015

The newly formed Knowledge and Information Executive Group (KIEG) had a defined escalation route up to Executive Management Board.

It was due to be attended by representatives from Home Office Directorates and Arm's Length Bodies, as well as subject matter experts from Home Office Technology, Corporate Security and the Office of the Chief Digital Officer.

The Houses of Parliament 2016

An endorsed customer service charter set expectations for the KIM team in terms of service standards and for the business in relation to compliance with policy.

Department of Health 2014

A quarterly 'Why Information Matters' newsletter for Local Folder Managers (LFMs) highlighted training sessions, news stories about forthcoming updates and improvements to the SharePoint IT system, requests for feedback, systems-related features and case studies.

Regular LFM sessions provide an opportunity to promote key priorities and answer questions and concerns.

HM Treasury 2015

The Information Management Steering Group was chaired by the DRO and Head of KIM. Membership included the CTO and reps from Internal Communications, IT Services, Knowledge Management, Site Owners, IT security and technical specialists.

Policy guidance and oversight

Providing direction

IMA Goal: The organisation gives staff the instruction they need to manage, protect and exploit information effectively

Providing guidance and supporting staff

Information management policy and supporting guidance should be up-to-date, relevant, proportionate, easy to understand and readily available. IT and other related guidance should deliver a single consistent message.

Once policy is defined it must be actively implemented. Available channels (from staff inductions to poster, leaflet or email campaigns) should be used to promote key messages and educate staff on the importance of information management.

‘Not having KIM as part of induction training means that the opportunity to set out what the standards are and what is expected of staff is missed’

IMA programme lessons learnt report

Policy guidance and oversight

Providing direction

Department for Work and Pensions 2014

Guidance was broken down into 'desk aids' to make it easier to understand and help staff have key principles to hand as they carry out their work.

Ministry of Justice 2016

Guidance was clear and succinct. It was clearly visible on the intranet and there were key KIM messages on the front page.

Retention and disposition schedules had been published in line with recommendations made by Sir Alex Allan in his 2014 *Records Review*. Retention schedules had been developed and updated in conjunction with business areas.

HM Treasury 2015

All staff were expected to complete face-to-face induction training in information and records management. Two sessions were provided.

One was run in the form of a quiz that conveyed key KIM messages and tested staff knowledge.

The other session gave a more formal, high-level view, addressing the business and compliance value of KIM. Key helpful tips included 'Don't be a slave to email' and 'Don't leave it until Friday, file as you go.'

Policy guidance and oversight

Measuring impact

IMA Goal: The organisation gives staff the instruction they need to manage, protect and exploit information effectively

Assessing compliance with policy

The Section 46 Code of Practice states that an information and records management policy should 'indicate how compliance with the policy and the supporting standards, procedures and guidelines will be monitored'.

If information and records management performance is understood, then bad practice can be addressed and behaviours can be challenged. Organisations can also identify and share good practice, encouraging others to raise their game.

Policy guidance and oversight

Measuring impact

HM Treasury 2015

Each business area scored KIM activities against a maturity model. Business areas that were not performing well had to repeat the process and, if they did not improve, had to meet with the Second Permanent Secretary to explain why.

Following benchmarking, business areas were expected to produce an action plan to demonstrate how they were going to improve.

Home Office 2015

The One3M model incorporated information assurance as well as information management. It was introduced to help embed good information management and encourage improved behaviours across the group.

Interviewees described One3M as ‘a flexible model that changes to accommodate new areas of focus’.

The Houses of Parliament 2016

A programme of health checks drew on face-to-face interviews with Record Officers and other relevant members of staff, and on systems usage statistics. This range of sources provided qualitative and quantitative insights into culture and performance: for example, a small volume of emails being stored could suggest that key context was not being captured.

Records review and transfer

Oversight of records and implementing disposal decisions

NOTE: If disposal activities have been put on hold, for example, to meet the requirements of the Independent Inquiry into Child Sex Abuse (IICSA), there must be a plan restart them at an appropriate point in the future.

IMA Goal: The organisation understands the value of its records and can consistently identify those with enduring historical value

IMA Goal: The organisation understands the process for records disposal and consistently implements decisions in line with defined plans

Records appraisal and disposal

The Departmental Records Officer (DRO) has lead responsibility for compliance with the Public Records Act.

Organisations cannot hold information indefinitely. Information in all formats that no longer has value should be destroyed, while information that has been selected for permanent preservation should be transferred to The National Archives or an alternative place of deposit once reviewed for sensitivity.

Records review and transfer

Oversight of records and implementing disposal decisions

Ministry of Justice 2016

Processes were in place to ensure that paper files were disposed of in line with agreed schedules: there was an annual destruction exercise each January.

Retention periods had been applied to the EDRMS and could be enacted. Requirements relating to existing disposal schedules had been factored into the move to the new, SharePoint based IT system.

Home Office 2015

The DRO was well-placed to exert influence on wider KIM issues, escalate risks and highlight issues.

The DRO reported to the Director of Performance and Risk who, in turn, reported to the Chief Operating Officer and Senior Information Risk Owner.

Welsh Government 2016 [progress review]

Welsh Government was a key participant in The National Archives' Digital Transfer Project pilots became the first organisation to transfer digital records to The National Archives.

Welsh Government demonstrated a willingness to engage, test The National Archives' processes and experiment throughout the project.