Information Management Assessment

A review of good practice from the IMA programme, 2008–14

Published:
September 2014

Working with government to raise standards in information management
## CONTENTS

**Introduction**  
2

- The value of information  
5
- Information and supporting technology  
10
- Information risk, governance and oversight  
14
- Records, review and transfer  
20

**Appendix A:** IMAs and progress reviews conducted  
24

**Appendix B:** performance framework  
26
INTRODUCTION

The Information Management Assessment (IMA) programme

The National Archives’ IMA Programme offers government departments and public sector bodies an independent and bespoke assessment of how well they are managing their information and records.

‘The IMA programme provides me, as Keeper of Public Records, with an assessment of whether the organisation is fulfilling its duties in relation to the Public Records Act. Not only is membership of the programme a highly effective way for an organisation to improve its information management, it also helps ensure that the decisions and life of that organisation today become tomorrow’s publicly accessible record.’

Jeff James, Chief Executive and Keeper, The National Archives

Individual assessments are risk focussed and positioned to gain a clear picture of an organisation’s policies, processes and practices. This entails consideration of governance arrangements, culture and the technology environment that staff are expected to use and work within. Onsite visits, scrutiny of documentation, a published report and further follow-up visits are designed to help improve standards and raise the profile of information management within member organisations.

In each case, we seek a statement of commitment from the head of the organisation to underline their support for our process and determination to drive good practice in information and records management. This should be published prominently on the organisation’s intranet or internet pages.

Demonstrating the importance of information and records Management

Cabinet Office

An example of a statement of commitment from Richard Heaton, Permanent Secretary of the Cabinet Office, taken from the department’s IMA report:

“The Cabinet Office holds some of government’s most important records, and as a department we are committed to making sure that we manage and protect them. An important part of our duty under the Civil Service Code is to keep accurate official records and handle information as openly as possible within the legal framework.

The National Archives regularly conducts assessments of Information Management practices and compliance within government departments, and to show the strength of our commitment to best practice I have asked them to review Cabinet Office processes and systems.

The following report will help me to support records management processes across the department, so that the right information can be appropriately captured, managed and preserved for the nation”.

IMA conducted August 2013
**Key outcomes**

After we produce a report, we work with an assessed organisation to support the creation of an action plan to address our recommendations. We then monitor the implementation of that action plan and produce a progress report.

Participating in the IMA programme helps public sector bodies to assess their ability to meet legal and policy obligations in relation to their information and records, with particular emphasis on the Public Records, Freedom of Information and Data Protection Acts. Further information on legal responsibilities can be found here.

Our assessments are also positioned to highlight the business benefits of protecting, managing and exploiting information effectively, and to help organisations to achieve them.

**Scope and structure of this document**

This document provides examples of good practice that have been identified in our reports, for the period 2008–14.

The examples that follow have been chosen to reflect the main areas covered in an IMA and are aligned to the current structure of our reports.

Each IMA report section asks a series of questions in relation to the organisations we assess.

<table>
<thead>
<tr>
<th>The value of information</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Does the organisation establish information’s value in principle and support its realisation in practice?</td>
</tr>
<tr>
<td>▪ Does the organisation protect, manage and exploit its information assets to achieve maximum value?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Information and supporting technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Does the technology environment support the management, protection and exploitation of information?</td>
</tr>
<tr>
<td>▪ Is the organisation taking proactive steps to ensure the continuity of its information, over time and through change?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Information risk, governance and oversight</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Is the organisation defining and managing information risks to minimise threats and maximise opportunities?</td>
</tr>
<tr>
<td>▪ Does the organisation have effective governance structures in place that foster</td>
</tr>
</tbody>
</table>
communication and strategic planning?

- Is the organisation giving staff the instruction they need to manage, protect and exploit information effectively?
- Is the organisation measuring performance in practice and taking informed risk-based action as a result?

Records, review and transfer

- Can the organisation understand the value of its records and can it consistently identify those with enduring historical value?
- Does the organisation understand the process for records disposal and consistently implement decisions in line with defined plans?

Further information and contact details


For further National Archive guidance on good practice in information management: How to manage your information

For more information on the Information Management Assessment Programme and its reports: Information Management Assessment Programme
1. THE VALUE OF INFORMATION

Public sector organisations need to provide an effective mandate for information and records management. To help support this, it is important to establish the value of information and communicate this to staff. To meet legal and policy obligations and to achieve the business benefits of good information management, organisations also need to ensure they are working to support the realisation of that value in practice.

The benefits of managing information

The successful management of information is an enabler for:

- efficient and effective delivery of services to government and to the citizen
- exploitation, sharing, use and re-use of an organisation’s information assets
- potential rationalisation of an organisation’s technology infrastructure
- efficient and effective use of the technology infrastructure
- transparency, accountability, citizen participation and legislative compliance
- the mitigation of the risk of loss of information within line of business systems and applications.

*Business requirements for managing digital information and records (2013)*

In order to assess how information is valued throughout an organisation, a typical IMA involves analysis of documentation and a large number of interviews, from non-executive board members to those with specialist IM or IT roles, and those who are expected to have embedded good information management as part of their every day work. A key consideration is whether senior staff and opinion formers are emphasising information management as a necessary activity that brings benefit to individuals and teams and to the organisation as a whole.

Organisations should recognise and position information as a "vital resource". This resource flows through the organisation - with its diverse objectives and strands of work - as well as its associated agencies and contractors. An endorsed and supported information strategy can help to ensure that key requirements are met and help drive increased capability and improved performance. For it to be effective, an information strategy needs to be comprehensive, time bound, agreed at a senior level and easily communicated. The action of drafting and publishing a strategy is, on its own, insufficient to embed its concepts. It needs to be actively adopted and regularly reviewed and should be accompanied by defined milestones and an implementation plan.

The IMA team has noted that approaches towards defining a strategy and vision for information have become more mature since the programme began in 2008. Best practice now shows organisations setting linked goals for the protection, management and exploitation of their
information and aligning these in support of overarching business objectives. Referencing and embedding the three core digital continuity concepts of availability, completeness and usability within a strategy can help promote a joined-up approach towards defined outcomes across a range of internal stakeholders.

In practical terms, the IMA programme recognises that a strong vision for the management, protection and exploitation of information can be supported through a robust information asset framework and a proactive approach in terms of enabling public access to information.

A number of the proactive initiatives undertaken by organisations that have been highlighted in IMA reports and progress reviews are listed below.

**Good information management is integral to business**

**Department for Business, Innovation and Skills (BIS)**

The BIS IMA report commended the department for establishing a draft KIM strategy and a clear vision that ‘KIM is not an added task, it is how we work’. The IMA report noted:

“The draft BIS Knowledge and Information Management strategy has the potential to act as a key driver for change, once endorsed and signed off. The draft strategy is aligned to the Information Principles for UK Government and establishes the importance of improving how knowledge is shared and how the value of information is understood and realised. It underlines the benefits of good practice in information management in terms of business outcomes, and in terms of compliance with department’s obligations under information legislation and the government’s transparency agenda”

*IMA conducted May 2013*

**High-level endorsement and regular review of an information strategy**

**Ministry of Defence (MOD)**

The significance of the Ministry of Defence’s Information Strategy (MODIS) was underlined by its publication on the department’s internet pages and by prominent senior-level endorsement from the Permanent Under-Secretary of State and the Vice Chief of Defence Staff. The MOD IMA report noted:

“MODIS establishes the Defence Information Vision and its status as an enabler of the main Defence Vision. It clearly establishes information as a strategic asset and the critical need for the department to transform the way it exploits it”

*Extract from MODIS:*
Telling staff why information management matters

Good policy effectively establishes roles and responsibilities. The Welsh Government IMA noted that the records management policy was published publicly and provided staff with clear direction on the importance of information, records and knowledge. Associated guidance highlighted the need to adhere to best-practice principles for records management and to store information correctly, sharing it appropriately and effectively. This was supported by a clear statement on the intranet:

“The knowledge and information we hold is one of our most important assets. It ensures that the decisions we make and the advice we give is based on a robust bank of evidence. Managing and protecting this information – particularly if it is sensitive or personal – is an important part of our role as civil servants.”

IMA conducted March 2014
"Knowledge is power"

The Department for Environment, Food and Rural Affairs (Defra)

A conference on the theme of "knowledge is power" was organised by Defra in order to raise the profile and skills of those business roles that are responsible for supporting and enabling better knowledge, data or information management.

The conference was targeted at senior leads and intended as a platform to underline the requirements for and benefits of good practice, and to launch a year-long programme of learning and development activities aimed at up-skilling staff.

IMA progress review conducted October 2013

Defining information assets at the right level

Department for Business, Innovation and Skills (BIS)

Information assets should be defined at a level that supports accountability and ownership and allows value, risk, content and lifecycles to be understood and managed. At the time of its IMA, BIS was reviewing its information asset management framework. The department’s report noted:

“BIS defines its information assets in an open and inclusive, best-practice manner … In line with the requirements of the Information Principles, this could support BIS to look beyond the provision of assurance on the security of information assets to enabling their effective management and exploitation”.

IMA conducted May 2013

Establishing an effective framework

The National Archives

The National Archives logs its information assets within an Information Asset Profile. This was established as a framework to enable the management, protection and exploitation of the organisation’s information assets. The National Archives’ approach was recognised as practical and pragmatic. The department defined its information assets on the basis of disposal schedules and explicitly included unstructured as well as structured information as a matter of course:

“Sample reporting summaries indicate that IAOs are required to provide assurance on a range of issues including application of retention. The model adopted is department specific, building on and exceeding Cabinet Office minimum requirements … As well as raising risks, IAOs are being asked to report on any steps they have taken to support transparency and detail efforts to increase the sharing potential of information assets”.

IMA progress review conducted October 2012
Gaining effective assurance from Information Asset Owners (IAOs)

Criminal Records Bureau (CRB)

CRB expanded the scope of its IMA to include retention. The department’s IMA highlighted how the agency had worked to empower its IAOs with a sense of ownership and responsibility:

“The Senior Information Risk Owner (SIRO) effectively delegated responsibility for management of risk to Information Asset Owners (IAOs) through the creation of an engaged network with support structures ... IAOs have quarterly meetings with the SIRO, complete quarterly returns, update the Information Asset Register (IAR) and are assigned administrators. Quarterly meetings actively engage individuals, with IAOs talking about their information assets and sharing best practice. IAOs reported feeling supported by the structure and IAO network, and the provision of administrative support demonstrated the recognition by CRB about the importance of the role”.

IMA conducted March 2012

Promoting the re-use of Information

The Environment Agency

Information assets have value within and outside organisations. The 2009 Environment Agency IMA report noted that the agency licensed a significant amount of its information to the business sector, the legal sector and the general public.

The Agency developed an "Approved for Access" programme to pre-assess categories of information it held, for example spatial flood risk maps. Categories of data and information that did not have such confidentialities could then be provided to the customer without further consideration.

This was an example of innovation and good practice with regard to the licensing of the organisation's information assets.

IMA conducted May 2009

Supporting the retention and exploitation of knowledge

Department for Culture, Media and Sport (DCMS)

Organisations need to manage and exploit knowledge as well as information. Following its 2010 IMA, DCMS took action to improve provision for knowledge capture and transfer when staff left or moved within the department:

“DCMS has recognised the need for better retention and sharing of corporate knowledge. Work in this area includes development of a handover report process to capture key role-specific information. It includes a section on file and records management. This document has been built into the Leaver’s checklist for development managers”.

IMA progress review conducted December 2012
2. INFORMATION AND SUPPORTING TECHNOLOGY

An effective technology environment is one that supports the management, protection and exploitation of an organisation’s information assets. It should be possible to manage digital information from creation to disposal and the technology environment should promote both the application of proportionate access controls and the routine publication of information.

Organisations need to encourage staff to capture and keep the right information in the right place and ensure that information can be retained as long as required, in line with its value. This includes the routine disposal of ephemeral information that has limited or no business value and no historical value, as part of a managed retention and disposal schedule. To support this, applications should perform consistently and systems should be low barrier and easy to use. Organisations also need to ensure that control and oversight can be exercised over alternative repositories.

As well as providing a supportive technology environment, organisations need to ensure the digital continuity of their information assets can be maintained over time and through change. **Digital continuity** is the ability to use digital information so that you can: find it when you need it; open it as you need it; work with it in the way you need to; understand what it is and what it is about; and trust that it is what it says it is, for as long as you need it.

In practical terms, organisations should, as a first step, define and document how they need to use their information assets and how this needs to be supported by technology. Both small- and large-scale procurement of new technology should be led by a clear understanding of business requirements and be supported by close collaboration between IT, information assurance and information management professionals and advisers. Organisations should also have a digital continuity plan in place. This can be used to ensure support and technical capability is provided where needed and to promote the achievement of business needs. In the long term, these will include the completeness, availability and usability of digital information with historical value that needs to be transferred to The National Archives.

What is digital continuity? The concepts of complete, available and usable information.
The IMA programme has identified a number of good-practice approaches undertaken by organisations in relation to their technology environments. These include both the provision and maintenance of corporate repositories and efforts to direct and shape how information is stored and exchanged.

<table>
<thead>
<tr>
<th><strong>Enabling routine information management processes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Welsh Government</strong></td>
</tr>
<tr>
<td>The Welsh Government provided a structured environment for the lifecycle management of digital and paper information through its Electronic Document and Records Management System (EDRMS), iShare. The Welsh Government IMA report noted work that had been undertaken to ensure the EDRMS continues to provide a supportive and enabling environment for records management:</td>
</tr>
<tr>
<td>“Retention schedules are applied at folder level and are being actioned according to defined triggers ... Welsh Government has sought to gain further benefit from its EDRMS by standardising processes such as file creation and naming, and the allocation of privileges. This has been achieved via the ‘Tasks’ workflow process. This effectively acts as a filter for requests from the business, supporting the consistent application of defined criteria”.</td>
</tr>
<tr>
<td><em>IMA conducted March 2014</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Taking control of shared folders</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Her Majesty’s Revenue and Customs (HMRC)</strong></td>
</tr>
<tr>
<td>HMRC developed a series of Controlled Access Folders (CAFs) to store case, policy and non-transactional data outside of duty systems and databases. These were introduced to replace shared folders in the shared drives. CAFs allow access to be restricted to discrete business groups or projects. The HMRC IMA report recognised that these had the potential to better manage the risk raised by the department’s previous shared folder structure.</td>
</tr>
<tr>
<td><em>IMA progress review conducted May 2012</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Personal drives: &quot;Identify the culprits&quot;!</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ministry of Defence (MOD)</strong></td>
</tr>
<tr>
<td>Reliance on personal repositories in preference to a shared corporate repository may undermine the availability of information and records and their completeness if key context cannot be found. The 2011 MOD IMA recognised the department’s efforts to address the issue of personal drive usage. In addition to the application of size limits, the assessment team noted a number of approaches including within Permanent Joint Headquarters (PJHQ) where:</td>
</tr>
</tbody>
</table>
“a proactive policy of ‘naming and shaming’ the worst offenders had been put in place to publicise the issue of records storage outside Meridio and drive people to review their personal drives.”

IMA conducted September 2011

Exercising control over alternative repositories

Criminal Records Bureau (CRB)

CRB launched a specific project to address the risks relating to storage of information in personal G Drives in preference to the Corporate File Plan (CFP):

“CRB is aware that the retention and storage of information has become an issue. Historically, CRB has not imposed a limit on the size of personal drives (G Drive). The ‘G Drive Project’ was introduced by CRB in recognition of the fact that some staff had been using their G Drives to store information and records in preference to CFP. The assessment team heard that this was due in part to the perception that CFP is time consuming and complex to use. The project aims to drive staff to move corporate information to the CFP by imposing a size limit of 250MB on G Drive personal storage space.”

IMA conducted May 2012

Driving routine engagement between KIM and IT

The National Archives

Joined-up governance for information helps support the achievement of digital continuity outcomes. The 2012 IMA of The National Archives highlighted improved alignment and closer relationships between IM and IT professionals:

“The Head of KIM sits on the IT strategy panel and leads on user engagement and information management themes. KIM team membership of the Technical Governance Board has the potential to influence the development of new IT projects. It allows the opportunity for KIM concerns to be raised so that they can be addressed and factored into system and application design”.

IMA progress review conducted October 2012

Building a common understanding

The Ministry of Justice (MOJ)

The MOJ IMA highlighted the need for closer formal relationships between IT and IM functions. MOJ has sought to address this concern, and the department’s progress review noted that the KIM team
now “has an ICT account manager embedded to drive better communications between the two functions”.

**IMA progress review conducted July 2012**

---

**Understanding what information assets you hold**

**Criminal Records Bureau**

Understanding what information assets you hold is a key first step in digital continuity planning:

CRB has recognised the need to identify information assets held within business areas and record these on the IAR. This has increased CRB’s oversight and ability to manage information and [it has] been safely able to dispose of information assets that are no longer required.

**IMA conducted November 2011**

---

**Planning to ensure the continuity of digital information**

**Department of Energy and Climate Change (DECC)**

Digital continuity is vulnerable at times of change, whether this is organisational, information management or technology related. The DECC IMA progress review noted the department’s creation of a tailored digital continuity plan ahead of the move to its new records system:

“DECC has written an internal two-page digital continuity strategy produced with a focus on the move to DECC Shares and the need to ensure metadata, and content are maintained when information is migrated between systems”.

**IMA progress review conducted January 2014**
3. INFORMATION RISK, GOVERNANCE AND OVERSIGHT

Organisations face numerous risks in relation to the information and records they hold and have responsibility for. Those relating to the security of information are often well understood. In the experience of the IMA programme, those relating to the management of information and records tend to be less likely to be defined formally, although the effect for an organisation may be no less significant.

Organisations should ensure that information and records management related risks are captured within their corporate risk management framework and that the potential threats to the completeness, availability and usability of information are understood. This may be leveraged through an Information Risk Management policy – one of the mandatory minimum measures promoted through the Security Policy Framework.

| Information risks related to governance and culture: Lack of comprehensive oversight and control |
|-----------------------------------------------|-----------------------------------------------|
| **Questions to ask**                          | **Potential sources of assurance**              |
| Does the Board understand the information risks facing the organisation as a result of its business activities? | Key information assets across the organisation identified (content and systems) |
| Has risk tolerance been set for information risk? | A Board-level senior information risk owner identified (supported by a team to manage the organisation’s information, and information risks) |
| Is the Board aware of the potential impact on business integrity should the confidentiality, integrity or availability of information be compromised? | An information asset owner named for each information asset (‘asset owners’ must consider content, not just systems) |
| Does the Board see information risk as a business issue (in business language)? | Risks of managing the different assets (in terms of their sensitivity, Data Protection/privacy issues, confidentiality, integrity, availability and other risks flagged in this guide) |
| Have you mapped what information you hold (paper, electronic, historical, current, case files, policy records etc)? Do you know where it is all kept? And how? | A robust and regularly updated risk register for the organisation’s information risks |
| Have you assessed the risks associated with each key asset (risks of inappropriate disclosure/ failure to disclose/tampering/loss/deletion etc)? | Regular monitoring of the risk register and compliance with the mitigation plans |
| Does this approach fit with your risk management for other business risks? | Compliance with legislation and key standards |
| Have you reviewed the Data Protection and privacy issues surrounding particular sets of data (personnel files, CCTV footage, etc)? | Strong links between the information management team and IT teams |
| Is it clear who owns and controls each asset? | Information management factored into business and system design processes |
| Are your information systems (containing your key assets) accredited? | Strong, regular engagement of the Audit Committee |
| Are you as clear on the processes for managing paper as you are on electronic content? Are you confident that these processes (transfer, storage, access) are sufficiently secure and robust? | Processes for regularly updating all of the above |

*Managing Information Risk: A guide for Accounting Officers, Board members and Senior Information Risk Owners, The National Archives, with Cabinet Office (2008)*
Other core organisational arrangements needed to support effective information and records management include the establishment of a governance framework. Within this, the appointment of a board-level champion is recognised as a potentially effective means of promoting good practice. At the other end of the scale, organisations may also benefit from the use of centrally led networks to support staff and drive the appropriate use of systems.

Information and records management teams should work to provide a defined service to the business and ensure staff receive clear instruction through policy, guidance and training. These should deliver a consistent message on what is required of staff, reflecting the technology environment and systems that are in use as well as the business and policy context that the organisation operates within.

Once policy, guidance and training are in place, it is important to ensure that adherence can be monitored so that concerns can be addressed and good practice can be identified and promoted. Organisations should seek to benchmark their performance and report progress towards strategic goals so that risks can be managed and benefits can be demonstrated.

**Defining the risks**

**Ministry of Defence (MOD)**

If risks are not defined formally, they cannot be managed consistently. MOD was one of the few departments to identify 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 framework:

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

*IMA progress review conducted June 2014*

**Establishing an information risk policy**

**Cabinet Office**

Information risk and information security policies provide an opportunity to underline the impact of good and bad practice in information and records management. The Cabinet Office IMA noted the provision of a clear policy line to support understanding:

“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 and 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 it is no longer required”.

IMA conducted August 2013

Highlighted priorities to staff

Department for Education [previously Department for Children, Schools and Families (DCSF)]

When key risks have been identified, it is important to ensure they are conveyed to staff. In 2009, DCSF was found to be using a number of ways to promote good information assurance practices, such as alerts on the Intranet, which reinforced the message. This helped promote understanding among staff of the need for security and why it was a high priority.

IMA conducted July 2009

Appointing a knowledge and information management "champion"

Foreign & Commonwealth Office (FCO)

The 2009 FCO IMA highlighted the need for a formal structure for information management and for a high-level body to provide ownership and strategic direction. Among a number of developments highlighted since the original assessment, the 2012 IMA progress review noted that:

“FCO has a new records and information management governance structure that includes an Information Management Steering Group, chaired by the Chief Operating Officer (COO). The COO is the new Board level champion for knowledge and information management (KIM)”

IMA progress review conducted February 2012

Promoting joined-up governance

UK Export Finance (UKEF)

Governance boards are a key means of promoting a consistent approach for information management and assurance and supporting technology. The UKEF IMA report noted:

“The Information Security and Assurance Committee (ISAC) acts as the main governance body for information related matters, with a focus on information security and assurance, but including information and records management. The DRO is a standing member with the IT Director and Digital champion. The committee has a recognised function within the department’s control framework”.

IMA conducted January 2014
Local Information Managers can really make a key difference

Department for International Development (DFID)

DFID was commended in its 2008 IMA for the introduction of the role of the Information Manager (IM). Many IMs were making a valuable contribution to the organisation wherever they were located. The IMs held an annual IM forum where they met to discuss issues.

One of their key roles was as a local expert in the EDRMS, and in some cases they were seen as pivotal to how an office operates. DFID monitored how its EDRMS system is used on a quarterly basis. IMs took the lead in quarterly information audits of how the EDRMS system was being used by reviewing “the number of documents saved to [the system], their sizes, types of documents and naming conventions applied”.

IMA conducted November 2008

Helping to promote compliance and encourage good practice

HM Treasury (HMT)

The HMT IMA highlighted the use of Folder Controllers and Knowledge Champions as a form of first-line support for the Central Information Management and Records Unit, noting:

“They promote compliance with administrative standards and encourage good performance against knowledge management targets for succession planning and knowledge sharing.”

IMA conducted November 2010

Redefining support roles and re-energising networks

Department for Transport (DfT)

On-going effort is required to maintain networks. 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 that the role of BRO was being redefined to “address the need for a more efficient, skilled and supported network”. DfT was also commended for producing a specific tailored BRO toolkit to support BROs and their managers.

IMA progress review conducted February 2011
Introducing an "Information Management Passport"

Organisations should build on policy and seek to raise standards and educate staff on the importance of information and records management. MOD introduced a "Defence Information Management Passport". This was intended to educate staff and raise standards in records and information management. It consisted of an e-learning package called "Information Matters" and an accompanying scored questionnaire. The passport received high-level backing from the Second Permanent Secretary. It was rolled out according to business need across the department.

Two locations visited on the IMA made completion of the Information Management Passport mandatory before assumption of duties.

IMA conducted September 2011

Private Office records

Department for Environment and Climate Change (DECC)

There are two models for the management of Private Office papers, the second of which requires the business to register records. DECC supported this policy by only accepting submissions in the form of a link to a file stored in the department’s EDRMS, Matrix. Other departments assessed have added a standard message to Private Office email footers reminding staff of their obligations to register records.

IMA conducted March 2012

Conducting information health checks

The Department for Environment, Food and Rural Affairs (Defra)

Organisations can gain greater oversight and understanding of information and records management performance through conducting targeting performance within key parts of the business. The 2013 Defra progress review noted the departments on-going efforts in this area:

“Information audits, which received strong support in the IMA report, have been replaced by a system of [lighter touch] information health checks aimed at incentivising staff themselves to improve the management of knowledge and information at the local level. These reviews are conducted jointly by knowledge partners in the knowledge services team at the request of business”.

IMA progress review conducted October 2013
| Using metrics to support implementation of an EDRMS and to monitor its usage |
| Department of Energy and Climate Change (DECC) |

The 2014 progress review of DECC noted the continued production of monthly statistics on the usage of their EDRMS system. These were published on the intranet and reported at a local level. These charted the number of non-users versus active users and could identify areas of the organisation where use of the system was low.

Statistics of this kind can help to target further action or training to create improvements or cultural changes in particular directorates.

*IMA progress review conducted January 2014*
4. RECORDS, REVIEW AND TRANSFER

The Information Management Consultants (IMC) team at The National Archives supports the Keeper in their responsibilities for the supervision of government departments in the selection and safe-keeping of records, as required under the Public Records Act.

The IMC team liaises with government departments to advise and support them in the management of their information throughout its life-cycle, and advises on the selection of records, paper and digital, for transfer to The National Archives for permanent preservation.

The IMA programme supplements this work and pays specific attention to how organisations are planning to meet their obligations including under the 20-Year Rule.

Within government organisations, the Departmental Records Officer (DRO) has lead responsibility for compliance with the Public Records Act. Key requirements for a successful DRO include good working relationships with a range of stakeholders and an active role in raising risks and championing good practice. In overall terms, a DRO needs to assume responsibility for ensuring information is managed through its lifecycle, selecting information with historic value for permanent preservation and ensuring it is transferred at the appropriate time.

Selecting and transferring records: guidance published by The National Archives
The IMA programme examines whether organisations understand what records they hold and looks at the processes they have in place to support their safekeeping. As third parties are often involved in managing and storing information, organisations that are following good disposal procedures will audit and monitor secure disposal of their own records and those of organisations that share or produce records on their behalf.

Organisations should be in a position to undertake routine and value-based disposal decisions and should clearly define their requirements for sensitivity review. Sensitivity review should be carried out to identify whether any material is too sensitive to transfer to The National Archives, or needs to be transferred to The National Archives as closed because Freedom of Information (FOI) exemptions apply. As a component of this, organisations should ensure they have considered requirements for consultation with other bodies that may be affected and for redaction if parts of the material could be released with sensitive components redacted.

A number of the proactive initiatives undertaken by organisations that have been highlighted in IMA reports and progress reviews are listed below.

**Inspiring staff on the relevance and importance of the "Record" within their own organisation**

**Cabinet Office**

The Knowledge and Information Team at the Cabinet Office is led by the DRO. The department’s IMA report noted that the team was working to encourage good records management by engaging its staff on historic records, including preview days of records that are about to be transferred and opened at The National Archives. A series of "Behind Closed Doors" leaflets highlighting archival documents were also produced for staff.

*IMA conducted August 2013*

**Supporting disposal for digital records**

**The National Archives**

The National Archives’ IMA report highlighted the department’s 2010 “What to Keep” exercise, which provided a basis for the definition of retention schedules. The organisation had worked to apply these to its file plan and had begun the process of closing files within its EDRMS, prompting the start of the retention periods. The choice and consistent use of triggers for retention periods are crucial to ensuring that routine disposal can happen in practice.

*IMA conducted March 2011*
Appraising the value of records

Welsh Government

Appraisal processes centre on the identification of current or on-going business value and secondary, historical value. The Welsh Government IMA highlighted the provision of a clear statement on guiding principles within its macro appraisal policy:

“The records selected for permanent preservation should provide information about, and evidence of, what the Welsh Government has done and why, what it and its staff and management (Permanent Secretary, Head of Departments & Boards) have achieved, and of its impact locally and in the wider world. The selection process should also facilitate the survival of records which contain unique information incidental to their main purpose or function but which, nevertheless, might have research value.”

IMA conducted March 2014

Conducting digital appraisal

Welsh Government

The Welsh Government IMA highlighted work by the records team to begin in-life digital appraisal in addition to paper appraisal, noting:

“This proactive good practice approach is an important step in identifying historic value as early as possible in a records life”.

IMA conducted March 2014

Tools for digital appraisal of electronic records

Department for Business, Innovation and Skills (BIS)

BIS developed the Electronic Records Appraisal project, which recognised the need to dispose of digital files when they were no longer needed, as well as marking files for The National Archives without performing a file-b-file review. This approach was signed off by The National Archives’ Records Decision Panel and a set of criteria was developed by which BIS could search its EDRMS for folders that were likely to be of interest.

IMA conducted May 2013
Reviewing the paper record on a regular basis

Department for Communities and Local Government (DCLG)

The DCLG IMA highlighted a long-established system of macro review of paper records. The department’s IMA report noted that macro review was:

“conducted by staff with expertise and a comprehensive set of documentation to guide record selection decisions. The review team have for a number of years undertaken selection review at 25 years and there is good communication of review decisions with the Information Management Consultant from The National Archives ... [This] will help to absorb some of the capacity pressures of meeting targets for the 20-Year Rule change.”

IMA conducted March 2012

Providing context to transferred files and planned reduction of legacy records

Department for Business, Innovation and Skills (BIS)

BIS has traditionally engaged with The National Archives when seeking sign off on paper files identified as having historical value that may merit permanent preservation. BIS made use of a second review summary form, which it presented with lists of review decisions. This provision of additional context to review decisions was highlighted in the department’s report.

BIS also successfully reduced its legacy of paper records due for transfer to The National Archives. Work was carried out in the course of the transition from an in-house paper store to one provided by the department’s contractor. A large-scale transfer was successfully carried out alongside business-as-usual work.

IMA conducted May 2013
Appendix A: IMAs and progress reviews conducted

The IMA programme began in 2008 with an assessment of the Department for International Development. In 2012/13 we reviewed the structure and focus of our reports to ensure the programme continues to serve as a best-practice model for information and records management across government. The IMA programme is conceived as a rolling series of assessments – the first IMA reassessment took place in July 2014 with a revisit to Foreign and Commonwealth Office.

The list below reflects the IMA programme’s interactions with government organisations at the time of the good practice report’s publication.

2008
Department for International Development IMA

2009
Ministry of Defence Spot IMA
Environment Agency IMA
Department for Transport IMA
Department for Children Schools and Families IMA
Foreign and Commonwealth Office IMA

2010
Department for Culture, Media and Sport IMA
HM Revenue and Customs IMA
Ministry of Justice IMA
HM Treasury IMA

2011
The National Archives IMA
Department of Energy and Climate Change IMA
Department for Environment, Food and Rural Affairs IMA
Ministry of Defence IMA
Criminal Records Bureau IMA
Department for Transport IMA progress review
2012
Department for Communities and Local Government IMA
Foreign and Commonwealth Office IMA progress review
Department for Culture, Media and Sport IMA progress review
Ministry of Justice IMA progress review
The National Archives IMA progress review

2013
Department for Business, Innovation and Skills IMA
Cabinet Office IMA
HM Revenue and Customs IMA progress review
Department of Environment, Food and Rural Affairs IMA progress review

2014
UK Export Finance IMA
Welsh Government IMA
Foreign and Commonwealth Office IMA reassessment
Department of Energy and Climate Change IMA progress review
Department for Communities and Local Government IMA progress review
Ministry of Defence IMA progress review

Forthcoming assessments:

- The Department of Health IMA is scheduled for October 2014
- The Department for Work and Pensions IMA is scheduled for March 2015
Appendix B: Performance framework

Our performance framework establishes a set of indicative criteria for each of the ten headings under which we assess organisations, progressing through four different levels of maturity. These levels of maturity can be interpreted as follows.

- **Development area:** indicates a key issue or gap in process or governance that may trigger a range of risks for the organisation.
- **Satisfactory:** indicates an approach that is positioned to support efficiency and effectiveness and compliance with legal obligations and responsibilities.
- **Good:** indicates an approach that goes beyond mandatory minimum measures and reflects wider concerns. Activities are routine and consistent, proportionate and well supported.
- **Best practice:** indicates an approach that is mature, ambitious and embedded. Activities are embedded within wider business process and positioned to deliver/demonstrate recognisable benefit in line with business objectives.

Overall ratings in our reports reflect a consolidated view of performance across the criteria for each heading. Emphasis is given to good practice that should be recognised and promoted, and to concerns that organisations need to recognise and address.

This document draws on a range of source material including the Lord Chancellor’s Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000 and ISO15489; mandatory minimum measures and associated guidance set out in the Security Policy Framework; ICO guidance on the application of the FOIA; the Open Data Principles; and the Information Principles for the UK Public Sector. It also draws on good practice guidance promulgated by The National Archives, including Business Requirements for Managing Digital Information and Records and digital continuity guidance (such as Identify Information Assets and Business Requirements, Embedding Digital Continuity in Information Management and Incorporating Digital Continuity into your IT Strategy) and on the selection and transfer of records.
## SECTION 1: THE VALUE OF INFORMATION

### 1.1 Communicating and Realising Value

**Goal:** The organisation establishes information’s value in principle and supports the realisation of value in practice

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Development area</th>
<th>Satisfactory</th>
<th>Good</th>
<th>Best practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting direction</td>
<td>The organisation recognises the need to set goals for information management, but it does not yet do so at a strategic level.</td>
<td>The organisation has set time-bound strategic goals for information management. These are positioned to support compliance with legal obligations and responsibilities.</td>
<td>The organisation has a mutually supportive strategy/vision for the protection, management and exploitation of information. It sets proportionate goals to address key risks and improve capability and culture.</td>
<td>The organisation has established its information strategy/vision as an integral part of wider corporate strategy/vision. It is subject to regular review and is recognised as a key enabler of business outcomes.</td>
</tr>
<tr>
<td>Telling staff why information matters</td>
<td>The organisation recognises that the information it holds and works with has value, but it does not yet define this formally for staff.</td>
<td>The organisation defines the value of information for staff in information management policy. This emphasises legal obligations and responsibilities.</td>
<td>The organisation defines the value of information and required behaviours consistently across supporting and linked policy and guidance.</td>
<td>The organisation ensures that the value of information is defined through standard business processes. Key messages are promoted by senior staff and managers.</td>
</tr>
<tr>
<td>Publishing and enabling access to information</td>
<td>The organisation recognises the need to realise the value of its information, but its performance is variable in opening up access to it and publishing transparency data.</td>
<td>The organisation has put in place a framework that supports it to meet required standards in opening up access to information and publishing transparency data.</td>
<td>The organisation has a consistent overall approach to transparency, open data and enabling access to information that is linked to its information strategy/vision. It publicises its commitment.</td>
<td>The organisation establishes good information management as an enabler for transparency and open government. It engages with citizens and proactively publishes information unless there is an overriding reason not to.</td>
</tr>
</tbody>
</table>
### SECTION 1: THE VALUE OF INFORMATION

#### 1.2 Managing Information as a Valued Asset

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

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Development area</th>
<th>Satisfactory</th>
<th>Good</th>
<th>Best practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining information as an asset</td>
<td>The organisation recognises the need to manage its information as an asset, but it defines and categorises information assets at too high or too low a level of granularity.</td>
<td>The organisation’s definition of an information asset reflects Security Policy Framework requirements and is at a level of granularity that supports oversight and management.</td>
<td>The organisation’s definition of an information asset is interpreted consistently across supporting and linked policy and guidance. It encompasses unstructured and structured information.</td>
<td>The organisation’s definition of an information asset is fully embedded within the business. It provides a basis for effective governance and staff use it to describe the information they hold and work.</td>
</tr>
<tr>
<td>Establishing ownership of information assets</td>
<td>The organisation recognises the need to identify its most sensitive and valuable information assets, but it has not yet done so, or established who owns them.</td>
<td>The organisation has identified its most sensitive and valuable information assets and established who owns them. IAOs are providing assurance against key risks and issues.</td>
<td>IAOs are appointed consistently across the organisation. IAOs understand their role and provide routine assurance on the protection, lifecycle management and exploitation of their information assets.</td>
<td>IAOs actively participate in the organisation’s plan to establish the right culture. IAOs work together to ensure information assets are fully utilised so that their value can be realised internally and externally.</td>
</tr>
<tr>
<td>Cataloguing information assets</td>
<td>The organisation recognises the need to catalogue its information assets, but it does so to a limited degree or at too high or too low a level.</td>
<td>The organisation uses a framework such as an IAR to catalogue information assets containing personal or business-critical information. Key sensitivities and handling requirements are captured.</td>
<td>The organisation catalogues a wide range of unstructured as well as structured information assets. It consistently captures context that supports effective management including value, risk, content and lifecycle.</td>
<td>The organisation’s approach to cataloguing information assets promotes understanding of all the information it holds and has responsibility for. Business requirements are captured in line with The National Archives’ Digital Continuity guidance.</td>
</tr>
</tbody>
</table>
### SECTION 2: INFORMATION AND SUPPORTING TECHNOLOGY

#### 2.1 The Technology Environment

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

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Development area</th>
<th>Satisfactory</th>
<th>Good</th>
<th>Best practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing digital information</td>
<td>The organisation recognises the need to manage digital information from creation to disposal, but corporate systems do not yet support lifecycle management.</td>
<td>The organisation has a defined corporate repository for the storage of information that supports lifecycle management. Control is exercised over alternative repositories and legacy holdings.</td>
<td>The organisation adopts a consistent approach to lifecycle management of information across a range of corporate systems. Information can be captured and retained or disposed of in line with a defined retention and disposal policy.</td>
<td>The organisation uses common standards and information management applications operate predictably. Corporate systems make minimal impact on information creators and information can be retained in usable form as long as required.</td>
</tr>
<tr>
<td>Finding, exchanging and exploiting digital information</td>
<td>The organisation recognises the need to discover and retrieve stored information, but search functions are unreliable and the technology environment introduces artificial barriers.</td>
<td>The organisation has ensured that search functions meet current business needs. It is reducing artificial barriers within the technology environment that might limit the exploitation of information.</td>
<td>Corporate systems are easy to use and navigate and are consistently structured. The provision of knowledge sharing tools supports the discovery and exchange of information across the network.</td>
<td>Corporate systems enable effective collaboration between internal stakeholders and with external partners. They promote information/work flows and provide automated routes for the publication of data.</td>
</tr>
<tr>
<td>Accessing digital information</td>
<td>The organisation recognises the need to ensure the security of sensitive information, but key systems lack appropriate controls.</td>
<td>The organisation has put in place controls in key systems where sensitive information is held, and in relation to removable media to protect against malicious behaviour.</td>
<td>Corporate systems consistently support staff to work with and process sensitive information safely, reducing the risk that alternative solutions will be used.</td>
<td>Corporate systems promote the protection of sensitive information from unauthorised disclosure, alteration and destruction through its lifecycle. Controls are flexible and make minimal impact on users.</td>
</tr>
</tbody>
</table>
### SECTION 2: INFORMATION AND SUPPORTING TECHNOLOGY

#### 2.2 The Continuity of Digital Information

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

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Development area</th>
<th>Satisfactory</th>
<th>Good</th>
<th>Best practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding what information is held</td>
<td>The organisation recognises that its information may be vulnerable due to its location, age or format, but it has not yet conducted an assessment or produced a digital continuity plan.</td>
<td>The organisation knows where its most valuable and sensitive information assets are stored and has identified vulnerabilities due to their age or format. It has identified key digital continuity objectives.</td>
<td>The organisation has taken proportionate steps to understand the contents of its file stores, conducting analysis and prioritising risks and issues. It has developed a digital continuity plan.</td>
<td>The organisation uses its understanding to inform decisions on application provision and infrastructure rationalisation. Digital continuity planning is helping drive the effective use and exploitation of current business information.</td>
</tr>
<tr>
<td>Understanding how technology supports usability</td>
<td>The organisation recognises that technology supports the usability of its information, but it has yet to identify key dependencies.</td>
<td>The organisation has mapped the key technical systems, platforms and processes that its most valuable and sensitive information assets require to be usable.</td>
<td>The organisation has documented at an appropriate level how technology supports its information assets to be usable. It has defined key information/work flows.</td>
<td>The organisation has embedded consideration of supporting technology within its information asset management approach; KPIs are set and the impact of changes is tracked.</td>
</tr>
<tr>
<td>Considering digital continuity ahead of change</td>
<td>The organisation recognises the need to consider business requirements for information management during IT change and procurement, but it has no formal means of doing so.</td>
<td>The organisation has established formal mechanisms to support consideration of business requirements for information management during major IT change and procurement.</td>
<td>The organisation ensures that IT change and procurement processes consistently factor in business requirements for information management. Meeting them is recognised as a core success criterion.</td>
<td>The organisation is maintaining its understanding of its business requirements for information management. Potential threats and opportunities relating to information assets actively inform decision making during change.</td>
</tr>
</tbody>
</table>
### SECTION 3: INFORMATION RISK, GOVERNANCE AND OVERSIGHT

#### 3.1 Recognising Information Risk

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

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Development area</th>
<th>Satisfactory</th>
<th>Good</th>
<th>Best practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance for information risk</td>
<td>The organisation recognises the need to provide leadership on information risk, but it has not yet established an appropriate governance structure.</td>
<td>The organisation has appointed a SIRO who is appropriately trained. It has put in place a security governance structure that provides accountability and leadership on information risk.</td>
<td>The SIRO and Board consistently and visibly sponsor and champion the management of information risk. They emphasise the importance of adherence to corporate policy and guidance.</td>
<td>The SIRO and Board prioritise the establishment of a reporting and learning culture. Senior staff and managers recognise their accountability and consistently promote the importance of managing information risk at all levels of the organisation.</td>
</tr>
<tr>
<td>Establishing how to manage information risk.</td>
<td>The organisation recognises that information risks may have significant impact, but it has not yet produced a definition or produced a policy for its management.</td>
<td>The organisation has produced a definition of information risk that reflects legal and regulatory requirements and has published an information risk management policy.</td>
<td>The organisation has defined tolerances, appetites, reporting lines and escalation routes. It consistently assesses risks to inform decisions on the management, handling and exploitation of information.</td>
<td>The organisation manages information risk within the standard business risk framework, and it is represented on risk registers at all levels. It is considered alongside and as a factor in other business risks.</td>
</tr>
<tr>
<td>Identifying causes, threats and opportunities</td>
<td>The organisation recognises the need to develop its understanding of information risk, but it identifies a narrow range of causes and has not yet documented it at an appropriate level.</td>
<td>The organisation has identified key information risks at a proportionate level. It recognises that information management as well as handling can be a significant source of risk for the organisation.</td>
<td>The organisation documents a proportionate range of threats raised by governance, planning, policy and practice in information management and handling. It identifies mitigating actions.</td>
<td>The organisation documents the risk of not sharing or exploiting information according to its value. It emphasises the potential strategic impact of such risks, focussing on opportunities as well as threats.</td>
</tr>
</tbody>
</table>
### SECTION 3: INFORMATION RISK, GOVERNANCE AND OVERSIGHT

#### 3.2 Establishing Control

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

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Development area</th>
<th>Satisfactory</th>
<th>Good</th>
<th>Best practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning and delivering a service to the business</td>
<td>The organisation recognises the need to allocate lead and operational responsibility for information and records management, but it has not yet done so.</td>
<td>The organisation has allocated lead and operational responsibility for information and records management. A plan to address key priorities has been developed.</td>
<td>The information and records management function has staff with the necessary KIM skills and a proportionate plan in place to provide support to the business, improve capability and address identified risks.</td>
<td>The information and records management function is positioned to provide crucial assurance to the board. It actively engages with the business and is responsive to emerging needs.</td>
</tr>
<tr>
<td>Ensuring information professionals support each other</td>
<td>The organisation recognises the need for communication between information and records management, IT and IA staff, but few formal channels exist.</td>
<td>The organisation has established formal channels that support communication and collaboration between information and records management, IT and IA staff.</td>
<td>Information management and records management, IT and IA staff are working together on a routine basis. Governance arrangements such as Board membership enable a co-ordinated approach.</td>
<td>Information and records management, IT and IA staff engage in joint planning at a strategic and operational level. Close working relationships ensure that a shared understanding is maintained.</td>
</tr>
<tr>
<td>Devolving responsibility to supporting networks</td>
<td>The organisation recognises the need to devolve administrative responsibility for information management, but it has not yet defined how it will do this in practice or allocated supporting roles.</td>
<td>The organisation has identified where it needs to devolve administrative responsibility for information management. Roles have been allocated to support compliance with policy and support the business.</td>
<td>The organisation is setting up networks and communities. These are well supported and are working together to enable the consistent protection, management and exploitation of information.</td>
<td>The organisation has well-established networks and communities in place. These are providing expert advice and have a recognised role in enabling operational efficiency and effectiveness.</td>
</tr>
</tbody>
</table>
### SECTION 3: INFORMATION RISK, GOVERNANCE AND OVERSIGHT

#### 3.3 Providing Guidance

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

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Development area</th>
<th>Satisfactory</th>
<th>Good</th>
<th>Best practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establishing policy to inform decision-making</td>
<td>The organisation recognises the need to provide policy and guidance for information and records management, but documentation is not current or easy to find.</td>
<td>The organisation has current, comprehensive published policy and guidance in place for information and records management. It is centrally hosted, easy to find and accessible.</td>
<td>Policy for information and records management exists within a wider framework that is mutually supportive and targets identified risks. It is endorsed by senior management and promulgated.</td>
<td>Policy for information and records management is aligned with information and business strategies. It is published externally and regularly reviewed to ensure ongoing relevance.</td>
</tr>
<tr>
<td>Identifying what to keep and how it should be managed</td>
<td>The organisation recognises the need to manage volumes of digital information, but it does not yet provide appropriate disposal guidance for staff.</td>
<td>The organisation has produced generic disposal guidance that establishes what information needs to be kept, where, by whom and for how long.</td>
<td>The organisation produces proportionate, tailored disposal guidance. It works with users to ensure guidance remains up-to-date and reflects key quality requirements.</td>
<td>Disposal guidance is recognised as a key corporate resource. Its use is promoted at all levels of the organisation as a means of mitigating risks to the availability and completeness of information.</td>
</tr>
<tr>
<td>Meeting training needs</td>
<td>The organisation recognises the need to ensure staff are aware of standards for information management, but it is not yet providing training.</td>
<td>The organisation has identified training requirements for information management. It is providing instruction to ensure staff are aware of standards and guidelines.</td>
<td>The organisation consistently engages senior staff and managers to increase understanding of good practice. It employs professional information management staff and supports their continuing development.</td>
<td>The organisation ensures that protecting and managing information are recognised as key competencies and embedded within induction processes at all levels. Training needs are evaluated on an on-going basis.</td>
</tr>
</tbody>
</table>
## SECTION 3: INFORMATION RISK, GOVERNANCE AND OVERSIGHT

### 3.4 Measuring Impact

**Goal:** The organisation measures performance in practice and takes informed risk-based action as a result

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Development area</th>
<th>Satisfactory</th>
<th>Good</th>
<th>Best practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establishing oversight to monitor performance</td>
<td>The organisation recognises the need to understand how information is being managed and handled, but lacks oversight and has not defined metrics.</td>
<td>The organisation has sufficient oversight of the technology environment to understand how information is being managed and handled within corporate repositories. It has defined a basic range of metrics.</td>
<td>The organisation has oversight of the majority of the technology environment. It has identified a proportionate range of metrics that can help it to understand how information is being handled, managed and exploited.</td>
<td>The organisation has oversight of the whole technology environment and it can obtain detailed metrics according to need, at all levels. It has identified a range of quantitative and qualitative performance measures.</td>
</tr>
<tr>
<td>Reporting performance</td>
<td>The organisation recognises the need to report performance in information management and handling, but is not yet defined requirements.</td>
<td>The organisation has defined when and how to monitor performance in information management and handling in line with its own needs.</td>
<td>The organisation routinely reports progress in information management and handling, emphasising progress to drive capability and manage risks. Performance is visible at Board level.</td>
<td>The organisation seeks continual assurance on performance in information management and handling and progress to achieve information strategy goals. It can demonstrate the business benefit of KIM in line with corporate objectives.</td>
</tr>
<tr>
<td>Targeting bad practice and driving up standards</td>
<td>The organisation wishes to increase capability in information management and handling, but has not yet established benchmarks.</td>
<td>The organisation has defined what good and bad look like in terms of compliance with legislation, regulatory requirements and key business outcomes. Responsibility for corrective action is allocated.</td>
<td>The organisation is using its understanding of performance in information management and handling consistently, to highlight good practice and prioritise areas for improvement.</td>
<td>The organisation uses tools such as information management improvement plans, maturity models and internal health checks on a structured basis; performance is assessed to drive continual improvement.</td>
</tr>
</tbody>
</table>
## SECTION 4: RECORDS REVIEW AND TRANSFER

### 4.1 Records Appraisal and Selection

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

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Development area</th>
<th>Satisfactory</th>
<th>Good</th>
<th>Best practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabling compliance with the Public Records Act</td>
<td>The organisation recognises the need to appoint a Departmental Records Officer (DRO), but it has not yet done so or defined its obligations under the Public Records Act.</td>
<td>The organisation has appointed the DRO role to oversee the management of information. It has defined its approach to addressing obligations under the Public Records Act.</td>
<td>The DRO role is positioned and supported to highlight key risks relating to records management. The DRO has a recognised role in leading on compliance with the Public Records Act.</td>
<td>The DRO role is integrated within wider systems of corporate governance. The DRO role plays a pro-active role in championing a culture of good information management.</td>
</tr>
<tr>
<td>Understanding volumes and value and managing resources</td>
<td>The organisation knows that its information is governed by the Public Records Act, but does not have an understanding of what it holds nor how to appraise its value.</td>
<td>The organisation can make a rough estimate of records held in all formats. It has identified roles and responsibilities required to meet its obligations under the Public Records Act.</td>
<td>The organisation can consistently determine the total volume of records it holds in all formats. It is able to judge the value of its records in line with key business objectives, functions and processes.</td>
<td>The organisation maintains its understanding of what information it holds, where and in what format. Its approach for records appraisal involves the business and is aligned with retention scheduling process.</td>
</tr>
<tr>
<td>Selecting records of historic value</td>
<td>The organisation recognises that its records may have value for the users of the future, but is not yet able to identify them or apply selection criteria.</td>
<td>The organisation has used generic selection criteria to develop its justifications for selection. It is investigating how to apply these to digital and hybrid records.</td>
<td>The organisation understands which records are likely to hold historical value, and is able to select them consistently in line with the policies agreed with The National Archives, using different methods to address different requirements.</td>
<td>The organisation has produced and published a clear description defining historical value, which is endorsed by The National Archives after public consultation. It selects records using the application of the agreed and justifiable criteria across all formats.</td>
</tr>
</tbody>
</table>
### SECTION 4: RECORDS REVIEW AND TRANSFER

#### 4.2 Implementing Disposal Decisions

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

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Development area</th>
<th>Satisfactory</th>
<th>Good</th>
<th>Best practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disposing of records securely</td>
<td>The organisation recognises that it needs to dispose of records, but has not yet defined how to do so across all formats.</td>
<td>The organisation has defined requirements for the secure disposal of records (including closed records). It is carrying out the secure destruction of records in all formats and maintaining an audit trail</td>
<td>The organisation has the resources and support to consistently implement approved value-based processes for the routine and secure disposal of paper and digital records in line with its disposal policies.</td>
<td>The organisation takes routine and auditable decisions on the disposal of all records in all formats with support from the business. It actively monitors performance of contractors to ensure criteria are met.</td>
</tr>
<tr>
<td>Reviewing records for sensitivity</td>
<td>The organisation recognises the need to conduct sensitivity review, but does not yet provide a trained and expert resource.</td>
<td>The organisation has defined its requirements for sensitivity review, including consultation and redaction. It provides a suitably trained and expert resource and ensures it applies to the Lord Chancellor’s Advisory Council in time to meet the 20 Year Rule.</td>
<td>The organisation has arrangements in place to determine routinely which records should be retained in the department, designated as open on transfer or transferred as closed. Exemptions are applied consistently across records.</td>
<td>There are proven, monitored processes in place for the sensitivity review of paper records and application of exemptions. The organisation is working with TNA to understand requirements for digital records.</td>
</tr>
<tr>
<td>Planning to transfer records</td>
<td>The organisation recognises its obligations to transfer records, but lacks a plan, or plans on an ad-hoc basis.</td>
<td>The organisation is working to a defined and agreed plan for records transfer to The National Archives and other places of deposit.</td>
<td>The organisation understands the impact of the 20-year rule on transfer volumes and has a proportionate plan in place to meet requirements covering all formats.</td>
<td>The organisation consistently meets the targets it sets and actively engages with The National Archives on the early transfer of records in all formats, where practicable and appropriate.</td>
</tr>
</tbody>
</table>
Visit our website to find out more about the Information Management Assessment programme and access copies of our reports:

http://www.nationalarchives.gov.uk/information-management/manage-information/ima/

The National Archives
Kew, Richmond, Surrey TW9 4DU
Tel: +44 (0)20 8392 4444

nationalarchives.gov.uk
@UkNatArchives

© Crown copyright 2014

You may re-use this document/publication (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence.

To view this licence, visit The National Archives website; or write to the Information Policy Team, The National Archives, Kew, Richmond, Surrey TW9 4DU; or email: psi@nationalarchives.gsi.gov.uk