The National Archives

Information Management Assessment

A review of lessons learned from the IMA programme, 2008–14

Published:

March 2015

Working with government to raise standards in information management

CONTENTS

INTRODUCTION

The Information Management Assessment (IMA) programme

The National Archives' Information Management Assessment (IMA) programme offers government departments and public sector bodies an independent and robust 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-focused and positioned to gain a clear picture of the effectiveness of an organisation's policies, processes and practices. We consider governance arrangements, culture and the technology environment that staff are expected 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 is published prominently on the organisation's intranet and internet pages.

Key elements of the IMA

Our assessments are designed to:

- help 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 on The National Archives' website.
- highlight the business benefits of protecting, managing and exploiting information effectively, and to help organisations to achieve those benefits;
- provide a robust and independent assessment of an organisation's information management capability.
- highlight examples of good practice and lessons learned that can be shared across government.

Following the IMA, we publish a report and work with the 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.

Scope and structure of this document

This report sets out the most common information and records management issues that The National Archives has found as part of our IMA Programme between 2008 and 2014. It also highlights some of the actions that can be taken to address these issues. It draws on the IMA reports, action plans and formal progress reviews that we have published on The National Archives website since 2009.

We have found that the organisations we assess are experiencing similar challenges to effective information and records management, which may undermine their ability to comply with legislation and government policy and to protect and exploit information for business purposes. These issues are not limited to the UK government. They are the same challenges that are being faced in information and records management in the wider public and private sectors in Europe and internationally.

Although this report focuses on the issues, it is important to stress that we have also found in the course of our assessments much good practice which we have highlighted in our IMA programme good practice report[1] published in 2014. All organisations assessed have put in place an action plan to address the issues found during their IMA, and the majority are making good progress.

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

The value of information

- Does the organisation establish the value of information in principle and support its realisation in practice?
- Does the organisation protect, manage and exploit its information assets to achieve maximum value?

Information and supporting technology

- Does the technology environment support the management, protection and exploitation of information?
- Is the organisation taking proactive steps to ensure the continuity of its information, over time and through change?

Information risk, governance and oversight

- Is the organisation defining and managing information risks to minimise threats and maximise opportunities?
- Does the organisation have effective governance structures in place that foster communication and strategic planning?
- Is the organisation giving staff the instruction they need to manage, protect and exploit information effectively?

[1] http://www.nationalarchives.gov.uk/information-management/manage-information/ima/ima-reports-action-plans/

- 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

For the Code of Practice (2009) on the management of records: Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000[2]

For further National Archive guidance on good practice in information management: How to manage your information[3] and information assurance[4]

For more information on the Information Management Assessment Programme and its reports: Information Management Assessment Programme[5]

For guidance from the Information Commissioners Office on obligations and how to comply with Data Protection and Freedom of Information Acts[6]

[2] https://www.justice.gov.uk/information-access-rights/foi-guidance-for-practitioners/code-of-practice
[3] https://www.nationalarchives.gov.uk/information-management/manage-information/
[4] http://www.nationalarchives.gov.uk/information-management/training/information-assurance-training/what-resources-are-available/
[5] http://www.nationalarchives.gov.uk/information-management/manage-information/ima/
[6] https://ico.org.uk/for-organisations/

EXECUTIVE SUMMARY

1. The value of information

Many of the organisations we have assessed do not have a clear understanding of the value of their information and the benefits of managing it effectively. Even where there have been efforts by the organisation's Knowledge and Information Management (KIM) team to define and communicate the benefits, they are often not recognised at senior levels and not fully understood by staff across the organisation. Organisations cannot effectively manage, protect and exploit information as an asset if they do not understand its value.

- **Senior support for information management will have a positive impact on the overall success of KIM initiatives and compliance with corporate policies.**
- **Having a clear process for the identification and management of information assets will enhance an organisation's ability to manage, protect and exploit its information.**

2. Information and supporting technology

Creating an effective and sustainable technology environment for the management of information and records remains one of the biggest challenges that government organisations face. Almost all of the organisations we assessed had ceased creating records by printing to paper and had been working 'largely' digitally since the middle of the last decade. Many experienced issues with the systems they used to manage their digital information. However, these issues were rarely to do with the technology itself and more about how the systems had been implemented and used. We also found that most organisations hadn't really planned for the continuity of their digital information in the longer term.

- **Fully considering your business needs and information management requirements when procuring systems to manage your digital information will lead to systems that support the way the organisation needs to work with its information.**
- **Decommissioning or properly managing other storage areas/systems such as shared drives when you roll out a new ERM system will enhance user take up and help to fully realise the business benefits.**
- **Properly managing email will ensure that key corporate information remains accessible and usable.**
- **Considering the digital continuity of your information will enable your organisation to work with its information for as long as it needs to.**

3. Information risk, governance and oversight

In many organisations, information risk assessment is interpreted in narrow terms with a focus on the security of information and data handling. Few organisations have fully defined risks relating to information and records management or formally recognise the impact of governance, culture and technology on performance. In overall terms, there is a need for a broader concept of information risk that covers completeness, availability, usability of information and can express the potential

outcomes of good and bad information management at all levels of an organisation. This should be supported by the recognition that good information management and good information security are interdependent and mutually reinforcing.

- **Fully understanding and managing risk at an appropriately senior level reduces the risk that information will become unavailable.**
- **Good information and records management governance and culture will enhance the success of KIM strategies and policies in practice.**

4. Records, review and transfer

Most organisations have a reasonably robust system in place for review and disposal of paper files, but few have developed an effective methodology or process for digital information. Organisations keep far more than they need. At the same time, information of real value to the organisation is often not recognised up front or saved in the designated corporate systems. Some organisations are therefore in breach of their obligations for the safekeeping and disposal of information under the Data Protection and Public Records Acts.

- **Understanding what information to keep and disposing of information when you no longer need it leads to business efficiency, decreased storage, maintenance and presentation costs and compliance with information legislation.**
- **Forward planning for appraisal, selection and transfer of records to The National Archives will enhance an organisation's ability to comply with its obligations under the Public Records Act, in particular the transition to the 20-year rule.**

1. THE VALUE OF INFORMATION

Many of the organisations we have assessed do not have a clear understanding of the value of their information and the benefits of managing it effectively. Even where there have been efforts by the organisation's Knowledge and Information Management (KIM) team to define and communicate the benefits, they are often not recognised at senior levels and not fully understood by staff across the organisation. Organisations cannot effectively manage, protect and exploit information as an asset if they do not understand its value.

Senior support for information management will have a positive impact on the overall success of KIM initiatives and compliance with corporate policies.

Summary of findings

- We have found during the course of our assessments that information and records management can be seen as less important to organisations than information assurance and information security. There has often been greater recognition of the need to comply with the Freedom of Information and Data Protection Acts or Data Handling requirements than the need to comply with the Public Records Act and adopt the Lord Chancellor's Code of Practice on the Management of Records. Good information management is an essential precursor to good information security: they are complementary.

- There is often a lack of understanding of why information management matters.

- Information and records management is often seen as an additional, burdensome task which is of secondary importance compared to the core business functions of the organisation.

- It is common for KIM Teams to have less influence within organisations than other areas, such as Information Technology or Information Assurance and KIM teams often find it difficult to compete for resources.

- The organisations we assessed often did not have a current, supported, strategic approach to increase understanding of information's value, improve standards of information management, and increase compliance with corporate policy. Even where strategy has been defined, it is rare for an organisation to integrate goals for information management and information technology.

What can be done?

- Where organisations do have a strategic approach to information management there are direct benefits, such as better exploitation of resources and reduced risk.

- Ensure that the role of good information management in enabling business outcomes is established consistently in policy and guidance and promoted to senior staff.
- Ensure that senior management understand the risks to the organisation of not managing information properly.
- Appoint senior staff to champion information and records management across the organisation, sponsor policy and support key initiatives.
- Ensure that strategic goals have been set to help improve standards of information and records management and ensure that these are linked to or embedded within IT strategy.
- Ensure that the information management strategy is aligned to the overall business strategy and obtain senior endorsement.
- Consider aligning information management and information assurance functions so these challenges are managed holistically.

Relevant guidance

- Understanding digital continuity[7] and what digital continuity means to you[8], which cover the benefits of information management, why it matters and what happens when information is not managed properly.

Having a clear process for the identification and management of information assets will enhance an organisation's ability to manage, protect and exploit its information.

Summary of findings

- Information Asset Registers (IAR) are often not being used to full effect. All the organisations we assessed had an IAR in some shape or form but many were either incomplete, not used consistently across the organisation or not kept up to date.

- Few organisations we assess are defining their information assets consistently or at a proportionate level. In some cases, information assets are being defined at too high a level, for example, listing a whole system as an asset rather the bodies of information that are held within it. This kind of approach is unlikely to support the provision of meaningful assurance or to provide a framework that promotes the effective management, protection and exploitation of information.

- In some organisations the KIM team had no involvement with the development or maintenance of IARs and they were not being used as a tool to aid information and records management.

- It is common for the Information Asset Owner (IAO) role to not be clearly defined or understood by staff in general and those who hold the role. We

[7] http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/step-by-step-guidance/step-1/
[8] http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/step-by-step-guidance/step-1/

found some confusion about the responsibilities and purpose of the IAO role and in some organisations reporting had been reduced to a box ticking exercise.

What can be done?

- Adopt a single definition of an information asset and ensure that it is recognised and understood across the organisation.
- Consider expanding IARs to document a wider range of context about information assets such as value, risks, purpose and disposal requirements.
- As far as possible ensure that IAOs have a direct business interest in the information assets they are responsible for.
- Ensure that the IAO role is assigned at an appropriate grade, clearly define responsibilities and ensure that these responsibilities are not delegated down. Make sure that the role is properly supported and recognised, for example, in annual performance reviews.
- Clarify IAO responsibilities in terms of unstructured data/records management
- Ensure that the relationship between IAOs and KIM networks/local information management networks is formalised.
- Ensure IAOs have a robust and regular reporting function e.g. to the Senior Information Risk Owner (SIRO) and are held to account.

Relevant guidance

- Identifying information assets and business requirements[9]
- Information assurance[10]

[9] http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/step-by-step-guidance/step-2/

[10] http://www.nationalarchives.gov.uk/information-management/training/information-assurance-training/what-resources-are-available/

2. INFORMATION AND SUPPORTING TECHNOLOGY

Creating an effective and sustainable technology environment for the management of information and records remains one of the biggest challenges that government organisations face. Almost all of the organisations we assessed had ceased creating records by printing to paper and had been working 'largely' digitally since the middle of the last decade. Many experienced issues with the systems they used to manage their digital information. However, these issues were rarely to do with the technology itself and more about how the systems had been implemented and used. We also found that most organisations hadn't really planned for the continuity of their digital information in the longer term.

Fully considering your business needs and information management requirements when procuring systems to manage your digital information will lead to systems that support the way the organisation needs to work with its information.

Summary of findings

- It is common for there to be a disconnect between IT and KIM professionals within organisations. KIM staff often felt that the importance of information management was not understood or taken into account by their IT colleagues. One outcome of a lack of join up between information management and IT strategies can be a lack of involvement of KIM teams in projects to procure and roll out new Electronic Records Management (ERM) systems. This sometimes had a direct impact on the success of the systems procured. Systems could not sufficiently perform basic information and records management functions that are essential to comply with the Data Protection and Public Records Acts, such as export of records and their metadata and disposal.

- Issues we found included deep and complex filing structures, complications with saving records into the system, the speed of systems, difficulties searching for information and confusion over having to 'declare' records. These sorts of problems had a direct impact on staff usage of ERM systems and therefore on operational effectiveness. This is why the information architecture should be designed by KIM professionals who have an understanding of information organisation.

- In some cases ERM projects were focussed on the technology outcome, for example, if we bring in X software it will solve our problems, rather than on defining requirements or goals for information and records and ensuring their achievement over the long term.

- Sometimes systems were selected because they were felt to be the cheap option or because the organisation was already using the software. In others it was because procurement was tied to a wider technical refresh that meant the organisation was driven towards a certain product and delivery timetable.

What can be done?

- Ensure that IT and KIM work closely together and ensure that there are representatives of both on projects to bring in new systems.
- Define your requirements for information management and test this against systems, for example, to ensure the system has a disposal or export function. You should also ensure that you can export records and their metadata in an appropriate format so you can migrate the data.
- Ensure that local information representatives and business areas are both involved when you are defining requirements, testing, selecting and piloting systems.
- Talk to software suppliers, get them to demo their systems, ask questions, challenge them – look beyond the sales pitch.
- Choose systems where records management functionality is automated and/or easy for staff to do.For example, where a new system has a function to 'declare records' or designate 'corporate value' consider not using this at all or applying it by default to certain types of records or in bulk to certain areas of the file plan to save the end user having to do so.
- During implementation, work with local information representatives and business areas to ensure that the chosen system works for them in practice. For example, work with business areas to create a filing structure that they can understand and use easily.

Relevant guidance

- Business requirements for managing digital information and records[11]
- Managing digital continuity[12]

Decommissioning or properly managing other storage areas/systems such as shared drives when you roll out a new ERM system will enhance user take up and help to fully realise the business benefits.

Summary of findings

- It is common for organisations to not decommission or limit the size of shared or personal drives after they had brought in a new ERM system.

- Many staff found shared and personal drives familiar and easy to use with recognisable team or personal filing structures and would use them in preference to the ERM systems. ERM systems, by contrast, were often reported to be slow, clunky and difficult to use.

[11] http://www.nationalarchives.gov.uk/documents/information-management/business-requirements-for-managing-digital-information-and-records.pdf
[12] http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/step-by-step-guidance/

- Where there were technical issues with ERM systems, there was usually a corresponding increase in the use of personal and shared drives. Even once the technical issues had been solved, staff often chose to stay away from the new system as they no longer trusted it.

- Where shared drives were being used, they were not always subject to central control and oversight. They were described as a 'wild west' with inconsistently named files and complicated and deep filing structures. While these may still allow individual staff members and teams to locate information, they make it incredibly difficult to find and share information from a corporate point of view (particularly after business change) or to impose business rules such as retention periods.

What can be done?

- Ensure there is a clear vision of the technology environment as a whole and the role/place of the ERM within it. Where alternative repositories are available (such as shared drives) an organisation should ensure it has enforceable and clearly communicated policy that sets out when, why and how they should be used.
- Switch off shared/personal drives. This should be a phased approach, usually with a period where staff can transfer information of business value to the new ERM and a period of read-only access before they are switched off. The process should be fully communicated to staff and they should be supported throughout.
- Make sure that staff know what to keep in line with corporate policies.
- Allow sufficient time for any unexpected technical issues to be addressed.
- Ensure that staff at all levels understand how to use your chosen corporate ERM and receive ongoing support through training and guidance. Ensure that new joiners receive training so they know what systems they should be using and how from the outset.
- If you retain shared and personal drives, ensure that they are managed in line with your other corporate systems.
- Reduce the size of shared and personal drives to incentivise staff to use corporate systems and do not, as a rule, increase the size of these drives.

Relevant guidance

- Managing digital records without an EDRMS[13]

[13] http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/managing-digital-records-without-edrms/

Properly managing email will ensure that key corporate information remains accessible and usable.

Summary of findings

- Some organisations had taken steps to reduce their email holdings and encourage staff to save emails of value to corporate systems, but email still posed a considerable challenge to most organisations we have assessed.

- Sometimes email was not recognised as part of the corporate record which meant that staff did not see a need to save them within the designated corporate repository.

- The effort required to move emails from the email system to the ERM system was often cited as a reason for leaving emails within inboxes or storing elsewhere. Some staff resented having to perform extra steps in addition to their daily work.

- Auto deletion and mailbox limits are not a solution in themselves. Some staff revealed that they worked around auto deletion periods by emailing themselves the information from their inbox again. Others circumvented inbox limits by saving emails en masse elsewhere, for example, by converting emails to PST files and storing them on their PCs. Mailbox limits were often extended, particularly for senior staff as KIM staff did not always feel empowered to push back on this issue.

- Some organisations had put email archives in place and in at least one case this had led to a huge archive containing 19 terabytes of email. Although this may reduce the burden on servers and staff in the short term, it is likely to prove extremely difficult to search, manage and dispose from in the future. This approach also raises the risk of non-compliance with legislation such as the Data Protection and FOI Acts.

What can be done?

- Ensure staff are clear on what emails they need to capture, who needs to capture them and when and where they need to be stored.
- Ensure that your chosen ERM system can be connected to your email system.
- Make it as easy as possible to move emails to the preferred corporate system.
- Consider bulk capture of emails, such as capturing whole inboxes.
- If an email archive is in place, ensure that staff understand the purpose of the archive and that emails of corporate value should still be saved to the appropriate corporate repository.
- Ensure that disposal is applied to email archives – don’t keep them indefinitely.
- Do not underestimate the importance of context – emails are easier to understand when accompanied by related records.
- Consider whether to limit the use of PST files by staff.

- There is no easy answer to the problem of email. It is largely about people knowing and wanting to do the right thing rather than technology or filing location.

Relevant guidance

- Managing emails[14]

Considering the digital continuity of your information will enable your organisation to work with its information for as long as it needs to.

Summary of findings

- Most organisations had not yet considered or made plans for their information requirements in the longer term to ensure that they can continue to find, open, work with, understand and trust their digital information. As the digital information they hold grows and ages this will increasingly become an issue.

- It was common for organisations to have an incomplete picture of their digital landscape both in terms of the digital systems in use and the information contained within them. It is difficult to ensure the continuity of information if you do not know what you hold or where. This is a particular risk at times of major change, for example, machinery of government changes.

- Some organisations had legacy digital systems but not all had taken steps to ensure that the information remained available in the long term.

What can be done?

- Actively plan for digital continuity as a component of or in alignment with information management strategy. Appoint a Senior Responsible Owner for Digital Continuity to champion digital continuity and coordinate work on this.
- Identify all those who have a responsibility for ensuring the continuity of digital information and ensure that this is recognised in their role and built into their day to day responsibilities.
- Take steps to understand your information, its value, how you need to use it and the nature of the technical and information environment that supports it and capture this in your IAR.
- Assess the risks to the digital continuity of your information and take actions to mitigate these risks.
- Embed digital continuity into business processes and strategies and ensure that it is factored into change projects, particularly technology or machinery of government changes.

Relevant guidance

[14] http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/managing-email/

- Digital continuity[15]

[15] http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/risk-assessment/

3. INFORMATION RISK, GOVERNANCE AND OVERSIGHT

In many organisations, information risk assessment is interpreted in narrow terms with a focus on the security of information and data handling. Few organisations have fully defined risks relating to information and records management or formally recognise the impact of governance, culture and technology on performance. In overall terms, there is a need for a broader concept of information risk that covers completeness, availability, usability of information and can express the potential outcomes of good and bad information management at all levels of an organisation. This should be supported by the recognition that good information management and good information security are interdependent and mutually reinforcing.

Fully understanding and managing risk at an appropriately senior level reduces the risk that information will become unavailable.

Summary of findings

- Some organisations did not have an Information Risk Policy, although the Data Handling Review established this as a minimum mandatory standard. Of those that had produced a policy, few had used it as an opportunity to define the place of information management-related risks within the wider risk management framework.

- We found in several organisations that information risks were not sufficiently visible and that there was not always a clear path for risks to be escalated to board level when required.

- In some organisations there was a lack of shared understanding of what information risk means. We found that information 'loss' is often defined as being about unintended disclosure rather than loss of availability, for example, around protecting sensitive personal data rather than ensuring that the organisation that the organisation can find, open, work with, understand and trust its information for as long as it needs to. Staff often told us they had difficulty finding information they needed which led to wasted time in searching or in doing the work again.

What can be done?

- Ensure your organisation has an Information Risk Management Policy and that it is used to set out how information management-related risks will be managed.
- Clearly define and communicate what information risks mean to the organisation and ensure that this covers risks around information availability and integrity as well as information security. Case studies are very helpful here.
- Ensure that information management risks are part of the wider risk management framework.
- Ensure that information risks are recognised and reported on at board level as appropriate so that progress in mitigating them can be understood and interrogated.

Relevant guidance

- Managing risk[16],
- Information assurance[17]
- Assessing risks to digital continuity[18]

Good information and records management governance and culture will enhance the success of KIM strategies and policies in practice.

Summary of findings

- Most organisations have clear, comprehensive guidance and policies. However, they are often not followed in practice, particularly when there is a poor culture of information management. The culture of an organisation has a direct impact on compliance with policy and the success and implementation of KIM initiatives. It is not enough to just have a good policy, implementation is essential.

- It is rare for there to be performance measures around information or records management activities outside KIM circles. This means that organisations may be unaware of areas of good practice that could be shared or built on, or bad practice that needs to be addressed.

- The solution to poor records management is not only or even mainly technical. The cultural or 'people' side is vital: education, training and a commitment to make it work.

- Where organisations had rolled out new ERM systems the cultural aspect was particularly important. Where this had not been properly addressed, take-up and acceptance of new systems was lower than expected. We found that a lack of enforcement from managers and a lack of staff understanding about why information management is important are key contributing factors in unsuccessful rollouts. Simply teaching people how to use the technology is not enough.

- We have seen some excellent examples of KIM induction training but in many cases it is not mandatory for staff to attend this. In some organisations KIM was not part of the induction training for new joiners. This has resulted in a lack of understanding among staff about their information management responsibilities and in inconsistent use of corporate systems for managing information. Not having KIM as part of induction training means that the

[16] http://www.nationalarchives.gov.uk/information-management/manage-information/managing-risk/
[17] http://www.nationalarchives.gov.uk/information-management/training/information-assurance-training/what-resources-are-available/
[18] http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/risk-assessment/

opportunity to set out what the standards are and what is expected of staff is missed.

- Most organisations we assessed had local information management representatives in place and over the years we have spoken to some very dedicated and committed people. However, many were not working to build and maintain an active network. The role is usually given to more junior members of staff with very little influence or support and responsibilities were often not clearly defined or part of performance objectives. It was common for the role to be an add-on to the main role; this limited the amount of time that could be spent on information and records management activities.

What can be done?

- Ensure that all staff understand their information and records management responsibilities both as a civil servant under the Civil Service Code and as a member of the organisation.
- Make it mandatory for all staff to attend KIM induction training.
- Incorporate information and records management activities into performance objectives for all staff.
- Local information management roles are crucial in improving understanding and practice of information and records management at all staff levels and extending the reach of the KIM team into the business. They can also be effective champions for good practice and help to unearth and flag concerns.
- Develop a centrally-led network of local information representatives and use it to champion good practice and promote standards.
- Ensure that local information management representatives are supported in their work through the management chain and that this is a recognised performance objective.
- When rolling out new systems, address the cultural aspects through regular and ongoing communication, training, guidance and workshops, and ensure senior staff lead by example.
- Ensure that guidance is consistent and easy for staff to understand and use, and in particular avoid information management jargon, and make guidance brief and to the point.

Relevant guidance

- How to manage your information[19]

[19] http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/risk-assessment/

4. RECORDS, REVIEW AND TRANSFER

Most organisations have a reasonably robust system in place for review and disposal of paper files, but few have developed an effective methodology or process for digital information. Organisations keep far more than they need. At the same time, information of real value to the organisation is often not recognised up front or saved in the designated corporate systems. Some organisations are therefore in breach of their obligations for the safekeeping and disposal of information under the Data Protection and Public Records Acts.

Understanding what information to keep and disposing of information when you no longer need it leads to business efficiency, decreased storage, maintenance and presentation costs and compliance with information legislation.

Summary of findings

- Staff often expressed confusion about what information they should keep. Occasionally, some staff would make fairly arbitrary decisions to delete information, but more often than not staff would resort to keeping everything 'just in case.' In one organisation, staff expressed the view that "all information can and should be retained." Many staff we spoke to had difficulty finding the information they needed. They often put this down to technical issues but in reality the problem was more likely to be a result of the sheer amount of information being retained as well as a failure to capture information in the designated corporate systems.

- Some organisations had produced guidance on what is a record and what to keep, but this was often found to be quite generic in nature or high level, leaving business areas to decide how this guidance applied to their own information. In some cases, staff were either not aware of this guidance or had never accessed it, in others staff were expected to "use their common sense" to decide what to keep. A failure to provide clear parameters in this regard increases the risk that the right information will not be captured or retained as long as needed. It also carries the risk that personal data will be kept for longer than needed.

- Attempts to appraise digital information in some organisations revealed the extent to which the wrong information was being saved within the wrong parts of the corporate systems or just not saved at all.

- Most organisations had not yet applied retention periods to, or started disposing of, their digital information. Even where retention periods have been identified, they were often not being followed through to conclusion. There is a disconnect between policy and practice.

- In some cases, retention had been applied to the main corporate repository but not to systems such as shared and personal drives or workflow systems. Within government all information is a public record under the Public Records

Act and should be managed as such. Records should be defined by their value and not by location.

- In more than one organisation the large amount of digital information kept in a system impacted on its performance, in particular search functionality. This not only affected the organisations' ability to carry out their business but also tarnished the reputation of the systems, leading staff to look for work arounds such as shared or personal drives.

What can be done?

- Work with business areas to understand what information they create, share and use and define why it is of value to the organisation and how long it needs to be kept.
- Record this information in a schedule.
- Produce clear and simple guidance on what to keep that is easy for staff to understand, for example, desk guides. In particular, try to avoid using information management jargon.
- Ensure that 'what to keep' is part of information and records management training.
- Ensure that the schedules and accompanying guidance are reviewed and updated regularly and appoint appropriate people to own this work.
- Use networks of local information managers to promote guidance on what to keep and to work with their business areas to ensure that they implementing the guidance properly.
- Consider condensing very granular retention schedules into broader catch-all retention periods. For example, one organisation used 8 years for all information unless an exception was identified. Another used short, medium and long retention periods of 3, 8 and 15 years.
- Automate the process of disposal where possible by building it into your digital systems.
- When procuring systems to manage digital information ensure that they have disposal functionality.
- Ensure that disposal is applied to all digital systems.

Relevant guidance

- Disposing of records[20]

Forward planning for appraisal, selection and transfer of records to The National Archives will enhance an organisation's ability to comply with its obligations under the Public Records Act, in particular the transition to the 20-year rule.

Summary of findings

[20] http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/disposal/

- In some organisations a failure to plan ahead meant they had a backlog of records awaiting appraisal, selection, sensitivity review and transfer. This is reflected in the Records Transfer Report figures that The National Archives has been collecting biannually since 2012.

- Some organisations experienced a 'bottleneck' effect with records being 'stuck' at a certain point in the process. In some cases issues around sensitivity review, such as deliberations over what exemptions may apply and the time it takes to redact sensitive information, meant the records could not progress to transfer. In others it was the physical preparation of records that was causing delay.

- In some cases organisations had outsourced certain aspects of the process such as cataloguing or preparation to third parties. Delays had occurred where the work was not being completed to the required standard.

- This is an area where resources are particularly stretched and in most organisations small teams carry out this work often alongside other duties. Delays were common when staff with knowledge and experience of this unique function moved to other roles or left the organisation. There was often a lack of forward planning to ensure knowledge transfer.

What can be done?

- Develop a clear picture of what is due for review and when, then work with your Information Management Consultant at The National Archives to devise a plan for the review of these records.
- Identify where delays in the process are occurring and devise solutions.
- Ensure that any third-party suppliers understand what is expected of them, have received necessary training and guidance and that their work is quality assured.
- Improve efficiency by considering methods of speeding up the process such as macro appraisal of records.
- Plan ahead for knowledge transfer when staff are due to leave this specialised function.

Relevant TNA guidance

- Selecting and transferring records[21]

[21] http://www.nationalarchives.gov.uk/information-management/manage-information/selection-and-transfer/

Appendix A: IMAs and progress reviews conducted

The IMA programme was fully launched in 2008 following a series of pilot assessments. The first full assessment was of the Department for International Development. In 2012-13 we reviewed the structure and focus of our reports to ensure the programme continued to serve as a best-practice model for information and records management across government. In 2015 we are reviewing our IMA strategy in response to a recommendation from Sir Alex Allan's report on Records Review. 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.

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

Department of Health IMA

Forthcoming assessments:

- The Department for Work and Pensions IMA is scheduled for March 2015.
- The Home Office IMA is scheduled for June 2015.
- The HM Treasury IMA reassessment is scheduled for September 2015.
- Department for Education reassessment is scheduled for November 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

Criteria	Development area	Satisfactory	Good	Best practice
Setting direction	The organisation recognises the need to set goals for information management, but it does not yet do so at a strategic level.	The organisation has set time-bound strategic goals for information management. These are positioned to support compliance with legal obligations and responsibilities.	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.	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.
Telling staff why information matters	The organisation recognises that the information it holds and works with has value, but it does not yet define this formally for staff.	The organisation defines the value of information for staff in information management policy. This emphasises legal obligations and responsibilities.	The organisation defines the value of information and required behaviours consistently across supporting and linked policy and guidance.	The organisation ensures that the value of information is defined through standard business processes. Key messages are promoted by senior staff and managers.
Publishing and enabling access to information	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.	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.	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.	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.

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

Criteria	Development area	Satisfactory	Good	Best practice
Defining information as an asset	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.	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.	The organisation's definition of an information asset is interpreted consistently across supporting and linked policy and guidance. It encompasses unstructured and structured information.	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.
Establishing ownership of information assets	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.	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.	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.	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.
Cataloguing information assets	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.	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.	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.	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.

SECTION 2: INFORMATION AND SUPPORTING TECHNOLOGY

2.1 The Technology Environment

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

Criteria	Development area	Satisfactory	Good	Best practice
Managing digital information	The organisation recognises the need to manage digital information from creation to disposal, but corporate systems do not yet support lifecycle management.	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.	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.	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.
Finding, exchanging and exploiting digital information	The organisation recognises the need to discover and retrieve stored information, but search functions are unreliable and the technology environment introduces artificial barriers.	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.	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.	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.
Accessing digital information	The organisation recognises the need to ensure the security of sensitive information, but key systems lack appropriate controls.	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.	Corporate systems consistently support staff to work with and process sensitive information safely, reducing the risk that alternative solutions will be used.	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.

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

Criteria	Development area	Satisfactory	Good	Best practice
Understanding what information is held	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.	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.	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.	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.
Understanding how technology supports usability	The organisation recognises that technology supports the usability of its information, but it has yet to identify key dependencies.	The organisation has mapped the key technical systems, platforms and processes that its most valuable and sensitive information assets require to be usable.	The organisation has documented at an appropriate level how technology supports its information assets to be usable. It has defined key information/work flows.	The organisation has embedded consideration of supporting technology within its information asset management approach; KPIs are set and the impact of changes is tracked.
Considering digital continuity ahead of change	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.	The organisation has established formal mechanisms to support consideration of business requirements for information management during major IT change and procurement.	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.	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.

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

Criteria	Development area	Satisfactory	Good	Best practice
Governance for information risk	The organisation recognises the need to provide leadership on information risk, but it has not yet established an appropriate governance structure.	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.	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.	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.
Establishing how to manage information risk.	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.	The organisation has produced a definition of information risk that reflects legal and regulatory requirements and has published an information risk management policy.	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.	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.
Identifying causes, threats and opportunities	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.	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.	The organisation documents a proportionate range of threats raised by governance, planning, policy and practice in information management and handling. It identifies mitigating actions.	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.

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

Criteria	Development area	Satisfactory	Good	Best practice
Planning and delivering a service to the business	The organisation recognises the need to allocate lead and operational responsibility for information and records management, but it has not yet done so.	The organisation has allocated lead and operational responsibility for information and records management. A plan to address key priorities has been developed.	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.	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.
Ensuring information professionals support each other	The organisation recognises the need for communication between information and records management, IT and IA staff, but few formal channels exist.	The organisation has established formal channels that support communication and collaboration between information and records management, IT and IA staff.	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.	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.
Devolving responsibility to supporting networks	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.	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.	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.	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.

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

Criteria	Development area	Satisfactory	Good	Best practice
Establishing policy to inform decision-making	The organisation recognises the need to provide policy and guidance for information and records management, but documentation is not current or easy to find.	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.	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.	Policy for information and records management is aligned with information and business strategies. It is published externally and regularly reviewed to ensure on-going relevance.
Identifying what to keep and how it should be managed	The organisation recognises the need to manage volumes of digital information, but it does not yet provide appropriate disposal guidance for staff.	The organisation has produced generic disposal guidance that establishes what information needs to be kept, where, by whom and for how long.	The organisation produces proportionate, tailored disposal guidance. It works with users to ensure guidance remains up-to-date and reflects key quality requirements.	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.
Meeting training needs	The organisation recognises the need to ensure staff are aware of standards for information management, but it is not yet providing training.	The organisation has identified training requirements for information management. It is providing instruction to ensure staff are aware of standards and guidelines.	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.	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.

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

Criteria	Development area	Satisfactory	Good	Best practice
Establishing oversight to monitor performance	The organisation recognises the need to understand how information is being managed and handled, but lacks oversight and has not defined metrics.	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.	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.	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.
Reporting performance	The organisation recognises the need to report performance in information management and handling, but is not yet defined requirements.	The organisation has defined when and how to monitor performance in information management and handling in line with its own needs.	The organisation routinely reports progress in information management and handling, emphasising progress to drive capability and manage risks. Performance is visible at Board level.	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.
Targeting bad practice and driving up standards	The organisation wishes to increase capability in information management and handling, but has not yet established benchmarks.	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.	The organisation is using its understanding of performance in information management and handling consistently, to highlight good practice and prioritise areas for improvement.	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.

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

Criteria	Development area	Satisfactory	Good	Best practice
Enabling compliance with the Public Records Act	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.	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.	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.	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.
Understanding volumes and value and managing resources	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.	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.	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.	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.
Selecting records of historic value	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.	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.	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.	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.

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

Criteria	Development area	Satisfactory	Good	Best practice
Disposing of records securely	The organisation recognises that it needs to dispose of records, but has not yet defined how to do so across all formats.	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	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.	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.
Reviewing records for sensitivity	The organisation recognises the need to conduct sensitivity review, but does not yet provide a trained and expert resource.	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.	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.	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.
Planning to transfer records	The organisation recognises its obligations to transfer records, but lacks a plan, or plans on an ad-hoc basis.	The organisation is working to a defined and agreed plan for records transfer to The National Archives and other places of deposit.	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.	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.