Information Management Assessment

The administrations of the Houses of Parliament

Reviewed
March 2016

Published
10th January 2017

Working with government to raise standards in information management
Contents

Statement of commitment 2
IMA background 2
Glossary 3
Key findings of the assessment 4
Highlights table 8
Recommendations to address risk areas 11

1 The value of information 15
2 Information and supporting technology 22
3 Information risk, governance and oversight 32
4 Records, review and transfer 45


You may use and re-use the information featured in this report (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence v3.0.

Any enquiries regarding the use and re-use of this information resource should be sent to psi@nationalarchives.gsi.gov.uk
Statement of commitment

The following statement was agreed in 2015 by the Senior Information Risk Owner (SIRO) of the House of Commons and the Director of Information Services in the House of Lords.

Statement of Commitment

Parliament recognises the importance of meeting its corporate obligations to effectively manage, protect and exploit its information.

To show the strength of our commitment we have asked The National Archives to review our processes and systems. The National Archives regularly conducts assessments of information management practices and compliance within government departments. The report they produce will help us to support all aspects of knowledge and information management across Parliament. It will help to make sure that our information, knowledge and records are appropriately captured, managed and preserved, and information risks and sensitivities are appropriately handled.

IMA background

The Information Management Assessment (IMA) took place between 14 and 17 March 2016. It focused on the management, protection and exploitation of information within the administrations of the House of Commons and the House of Lords. It also covered the Parliamentary Digital Service, which is a joint department of both Houses. Members and their staff are data controllers in their own right, and not subject to policies and governance relating to the management of parliamentary records. Members’ records were therefore excluded from this assessment.

The IMA entailed a detailed review of supporting documentation followed by interviews with senior staff, specialists and practitioners. These were conducted in person at the Houses of Parliament. The House administrations do not transfer
records to The National Archives. They are not subject to the Public Records Act and are not required to comply with the Security Policy Framework, but do follow supporting guidance for both. Consequently, the House administrations were assessed where applicable against the IMA Programme’s standard performance framework.

The report that follows provides a summary of good practice and risks identified. IMA reports and departmental action plans are published on The National Archives’ website at: nationalarchives.gov.uk/information-management/our-services/ima-reports-action-plans.htm

Glossary

ARDP – Authorised Records Disposal Practice
DRO – Departmental Records Officer
DROID – Digital Record and Object Identifier
EDRMs – Electronic Document and Records Management system
FOI – Freedom of Information
IA – Information Assurance
IAO – Information Asset Owner
IMA – Information Management Assessment
IRMS – Information and Records Management Service
KIM – Knowledge and Information Management
PDS – Parliamentary Digital Service
PST – Personal Storage Table
SIRO – Senior Information Risk Owner
SPIRE – The EDRMs used by the House administrations
Key findings of the assessment

1 The value of information

<table>
<thead>
<tr>
<th>Performance rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communicating and realising value</td>
</tr>
<tr>
<td>Managing information as an asset</td>
</tr>
</tbody>
</table>

- Unlike government departments, the House administrations are not subject to the Public Records Act and staff are not bound by the Civil Service Code. Nonetheless, information and records management practice broadly raises the same threats and opportunities as it does in government organisations.
- The benefits of managing, protecting and exploiting information are well expressed by the House administrations in policy documentation and guidance, but strategic goals and objectives have not been defined. This means that although teams with information-related specialisms are working well on an individual basis to ensure the value of information is realised, there is no overall framework and agreed set of goals to help co-ordinate and direct their work.
- There has been discussion of the benefit of embedding information and records management in the 2015 draft Digital Strategy, but this has not been actioned sufficiently. Key outcomes for information and records management would fit well within the strategy’s current structure, with more detailed planning drawn up in support.
- An Information Ownership Project has been set up to better understand what information business areas are holding. This has been conducted in keeping with key requirements set out in guidance published by The National Archives and Cabinet Office, including coverage of disposal criteria. The project has been subject to delays that have left some staff unclear about its status and aims. It offers considerable potential value to the two administrations and should be re-launched once the current stage is completed. There would be benefit in adopting a more joined-up approach for governance of sensitive and non-sensitive information assets to enable more consistent oversight.
2 Digital information and supporting technology

<table>
<thead>
<tr>
<th>Performance rating</th>
<th>Development area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supporting information through technology</td>
<td>Development area</td>
</tr>
<tr>
<td>Digital continuity and IT change</td>
<td>Development area</td>
</tr>
</tbody>
</table>

- An historic lack of joined-up planning between Information Technology (IT) and Knowledge and Information Management (KIM) staff has contributed to a lack of integration between current systems. There are limited controls in place to prevent staff from storing information outside the current Electronic Document and Records Management system (EDRMs), SPIRE, in locations such as email accounts. Microsoft Office 365 tools have been rolled out to some staff. While these are addressing a number of important user needs in terms of access to information, their use is currently undermining the benefit that SPIRE offers in terms of records storage.

- SPIRE utilises Meridio software and is due to be replaced in 2017. The House administrations have the opportunity to address many of the above issues and improve the availability of information through the Meridio Replacement Project and wider project to fully roll out MS Office 365. The relationship between the two needs to be formalised to facilitate this.

- The House administrations have made a start on identifying digital continuity objectives, but work was on hold at the time of the IMA. We recommend that the House administrations embed digital continuity principles in the Digital Strategy.

- IT Procurement processes have been overhauled recently. However, more needs to be done to ensure information and records management requirements are factored in routinely and that procurement and accreditation processes are engaged with.
3 Information risk, governance and oversight

<table>
<thead>
<tr>
<th>Performance rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recognising information risk</td>
</tr>
<tr>
<td>Establishing control</td>
</tr>
<tr>
<td>Providing guidance</td>
</tr>
<tr>
<td>Measuring Impact</td>
</tr>
</tbody>
</table>

- We gained a good level of assurance that the House administrations recognise the potentially significant impact of information risks, including those related to cyber-security.
- Information and records management related risks are visible to the Senior Information Risk Owners (SIROs) of both administrations. The two administrations have different frameworks in place for oversight of information risks and each has interpreted the risks that it faces in a different manner. They should consider how they can arrive at a more consolidated view of information and records management related risk, as has been achieved for cyber-security related risk.
- A number of information-related boards are in place. The Information Management Authority has a senior membership and links to the business and to information specialist staff through two separate sub boards, which gives it a potentially strong foundation. However, senior staff did not express full confidence in this arrangement at the time of our assessment. We recommend that the House administrations review the provision of information-related governance boards, with the proviso that information and records management requires an equivalent level of visibility in the future to that intended now.
- The Parliamentary Information and Records Management Policy is clear and has been well drafted. It goes further than a number we have reviewed in the past, produced by government departments, in setting out specific responsibilities for line managers and heads of departments/offices.
- Policy is supported by a range of good practice guidance and training. However, guidance is not always recognised or being followed by staff. The House
administrations must ensure that clear principles are established and sufficiently promoted to staff before and after the introduction of the new IT environment. This should be done as part of a defined plan to develop a supportive culture.

- The health check process set up by the Information and Records Management Service (IRMS) provides an overview of performance in information and records management through systems’ usage statistics and interviews with staff. Health check recommendations are positioned to improve performance, and business areas in need of support are directed towards the services offered by the team. In future, we recommend that line managers and heads of departments/offices are formally identified as key stakeholders so they can see how well they are meeting the requirements set out for them in the Parliamentary Information and Records Management Policy.

### 4 Records, review and transfer

<table>
<thead>
<tr>
<th>Performance rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oversight of records and selection</td>
</tr>
<tr>
<td>Implementing disposal decisions</td>
</tr>
</tbody>
</table>

- The current IT environment imposes some significant barriers to easy oversight of digital records; work currently under way, including the Information Ownership Project, is likely to help address this.
- The House administrations have a good level of understanding of the records held in SPIRE and appear to have control of their paper records. Clear criteria are in place to support appraisal and selection of records.
- The House administrations are disposing of digital information from SPIRE in line with their published Authorised Records Disposal Practice (ARDP). This places them some way ahead of a majority of government departments.
- Digital records have already been transferred to the Parliamentary Archives and testing for transfers from SPIRE is ongoing.
### Highlights table

The following are among the areas of good practice identified at the time of the assessment. They include systems and approaches that other government organisations may find helpful in mitigating information and records management related risks:

#### Highlights of the 2016 IMA

<table>
<thead>
<tr>
<th>Highlight</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The value of information</strong></td>
<td>Consistently highlighted in guidance and other documents we reviewed. The Information and Records Management Policy identifies good practice in information and records management as an enabling factor in compliance with the Freedom of Information and Data Protection Acts. It is also identified as a means of mitigating a range of risks, ranging from poor decision-making based on inaccurate information through to financial and legal loss. The policy was approved in 2014 at a senior level (Clerk of the Parliaments and Clerk of the House) and circulated to Board members of both administrations.</td>
</tr>
<tr>
<td><strong>The Parliamentary Information and Records Management Policy</strong></td>
<td>Is published on the parliamentary website in line with good practice principles set out in the S46 Code of Practice.¹ The House administrations have also published their Authorised Records Disposal Practice (ARDP) to show how decisions on retention and disposal are taken.</td>
</tr>
<tr>
<td><strong>The Information Ownership Project</strong></td>
<td>Has introduced a template Information Asset Register that covers key context including purpose, storage location and disposal. There are brief pointers under each heading to guide those populating it, with questions such as ‘Who has access to the information? How is access controlled?’ The project has adopted an open definition of an information asset that is not restricted to IT systems, personal data or significant datasets. Workshops have been held to encourage teams to think about how information flows between them. The creation of Information Asset Registers has encouraged some teams to rethink the sensitivity of their information assets and has resulted in new disposal schedules being defined.</td>
</tr>
</tbody>
</table>

The business case for the Meridio Replacement Project was developed with input from the business. Record Officers were consulted through 1:1 interviews and focus groups. A staff survey was also conducted to give feedback on the present system and find out what staff would like to be able to do that they cannot do with the existing technology.

The House administrations have conducted a number of initiatives aimed at mitigating cyber-security related risks from a technical and cultural point of view, including penetration testing and awareness campaigns on topics such as phishing emails. Information and records management related risk is visible to the Senior Information Risk Owner (SIRO) of both administrations.

The Parliamentary Archives' business plan is aligned to the strategic objectives of both administrations. The Information and Records Management Service (IRMS) has produced a Customer Service Charter, which was endorsed by the Business Management Group in the House of Commons and Business Planning Group in the House of Lords. It sets expectations for the team in terms of service standards and for the business in relation to compliance with policy.

The Parliamentary Information and Records Management Policy sets clear expectations for line managers and for heads of department/office. The latter are broadly responsible for strategic oversight and ownership of related risk, while the former are responsible for ensuring staff are aware of their responsibilities and have sufficient time available to them.

IRMS has a defined objective in place to develop Record Officer capability, awareness and skills. They are actively working to do this through a range of means including a programme of training, an annual general meeting, a quarterly newsletter, targeted emails and an annual Record Officer Desk calendar. This is a useful means of communicating helpful information and reminders of key requirements for the role. It includes key extracts from the Customer Service Charter and reminders on routine and date-sensitive activities that need to be undertaken. These range from setting retention trigger dates to reminding teams to review and clear out redundant emails. Key pieces of ‘how to…’ guidance are highlighted at the end.

Health checks draw on face-to-face interviews with Record Officers and other relevant members of staff, and statistics on systems usage. This range of sources provides qualitative and quantitative insights into culture and performance. IRMS can, for example, identify whether apparently good engagement with SPIRE is down to a team-wide ethic or to the action of a few team members. By looking at document types stored, IRMS can
also highlight where a relatively small volume of emails were being stored, suggesting that key context was not being captured.
Recommendations to address risk areas

Recommendation 1

Ensure strategic goals for the management, protection and exploitation of information are defined and agreed. Embed them within the Digital Strategy to support a comprehensive view of objectives and risks and enable co-ordinated planning.

This would be supported by:

- ensuring there is specific reference to ensuring the availability of records for the user of the future via the Parliamentary Archives
- embedding digital continuity outcomes within the strategy
- aligning the information risk approaches (including digital continuity) of both House administrations with the strategy and key objectives
- ensuring that a clear vision is in place for any supporting team business plans and implementation plans: this should integrate the work of IRMS with other teams and stakeholders.

Recommendation 2

Arrive at a single, consolidated approach for information asset ownership and governance that enables the management, protection and exploitation of sensitive and non-sensitive information assets.

This would be supported by:

- ensuring that the same context is collected about sensitive information assets as is currently collected for non-sensitive assets, as enabled by the Information Asset Register. For example, by adopting a single template Information Asset Register.
- reviewing the Information Asset Owner (IAO) role and setting clear expectations and requirements for owners of sensitive and non-sensitive assets
- establishing how IAOs will be supported in the provision of assurance – for example by their teams, by Record Officers or by other means.
### Recommendation 3

Formally define the relationship between the MS Office 365 roll out and the Meridio Replacement Project to enable joined-up planning and support effective use of resources.

We emphasise that SharePoint by itself does not currently deliver records management outcomes. Plug-ins are required to enable these.

This would be supported by:

- ensuring there is specific mention of the Meridio Replacement project in the Parliamentary Digital Strategy
- making shared use of The National Archives’ file profiling tool, DROID
- making shared use of the Information Asset Registers developed by the Information Ownership Project
- adopting a joint approach/vision for records storage and retrieval that encompasses the whole IT environment.

### Recommendation 4

Develop a specific plan to drive the effective use of systems and develop and embed a supportive Information Management culture in the new technology environment.

Implementation, roll-out and embedding work must be given the same priority as procurement if the benefits of the system that will replace Meridio and the wider IT environment are to be realised.

This would be supported by:

- ensuring that a fully revised charter and policy are in place to be launched in conjunction with the roll-out of the Meridio replacement
- gaining senior support to encourage compliance and promote a clear mandate
- gaining senior support to target key issues and problem areas, implementing a staged programme to reduce reliance on email and storage in personal repositories
- giving consideration to imposing proportionate technical restrictions
- producing and promoting a single suite of guidance for the new technology environment that integrates IM and RM requirements
- formally defining how compliance will be monitored
- identifying line managers and heads of department/office as key customers for compliance monitoring activities (such as outputs from the health checks): they would then understand how well their teams are meeting policy requirements.
<table>
<thead>
<tr>
<th>Recommendation 5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ensure the IT procurement process gives more consistent consideration to IM and RM requirements.</strong></td>
</tr>
<tr>
<td>This would be supported by:</td>
</tr>
<tr>
<td>• strengthening and communicating the mandate for adherence to the IT procurement and accreditation process</td>
</tr>
<tr>
<td>• establishing a documented risk management process</td>
</tr>
<tr>
<td>• ensuring that IRMS is identified as a stakeholder in general terms.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recommendation 6</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Review current provision of information-related governance boards to provide effective oversight of issues relating to the protection, management and exploitation of information.</strong></td>
</tr>
<tr>
<td>This would be supported by:</td>
</tr>
<tr>
<td>• ensuring agreed structures are strategically aligned</td>
</tr>
<tr>
<td>• defining how information will be championed at Board level.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recommendation 7</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Position policy, guidance, and Parliamentary Archives planning documentation to support the transition period before the new technology environment is introduced</strong></td>
</tr>
<tr>
<td>This would be supported by:</td>
</tr>
<tr>
<td>• adding short-term updates of the Information and Records Management Policy and Customer Service Charter to the 2016-17 Parliamentary Archives business plan</td>
</tr>
<tr>
<td>• adding a review of the Record Officer role and of IM/RM guidance to the Parliamentary business plan; recognising support roles such as this in performance reviews.</td>
</tr>
<tr>
<td>• formally defining how IRMS and the Head of IRMS (as Departmental Records Officer equivalent) support the SIROs of the two administrations²</td>
</tr>
<tr>
<td>• considering adoption of common data protection e-learning across both House administrations.</td>
</tr>
</tbody>
</table>

Recommendation 8

Strengthen controls around governance of paper records to ensure that common standards can be applied.

This would be supported by:

- defining the relationship between the Parliamentary Archives and any other archives – such as that held within the Parliamentary Estates Department – with a view to ensuring that records are protected and that the business has the access it needs
- establishing a means of tracking records loaned to, or held by, the business
- producing guidance on the identification and application of closure periods to documents.
1 The value of information

1.1 Communicating and realising value

Goal: The organisation establishes information’s value in principle and supports its realisation in practice.

Establishing the importance of information

The Parliamentary Information and Records Management policy is intended to enable a range of positive outcomes for the House administrations. These include increased efficiency and effectiveness, improved accountability and openness, the ability to protect information vital to the continued functioning of each House, and an ability to promote their achievements and contribute to Parliament’s heritage.

Good practice in information and records management is identified as an enabling factor in compliance with the Freedom of Information and Data Protection Acts. It is also identified as a means of mitigating a range of risks, ranging from poor decision-making based on inaccurate information through to financial and legal loss. The policy was approved in 2014 at a senior level (Clerk of the Parliaments and Clerk of the House) and circulated to Board members of both administrations. This is good practice.

The value that information has for the House administrations was consistently highlighted in the guidance and other documentation we reviewed, as noted throughout the body of this report. The importance that is attached to the management, protection and exploitation of information is clear from the effort invested in the various IA, IT and IM related workstreams currently underway.

We saw positive indications that key business areas such as the Restoration and Renewal programme have recognised the importance of working with the Information and Records Management Service (IRMS) and ensuring that records management is factored into the work they are doing. However, while staff generally recognise the value of the information they work with, the way in which it is managed and the extent to which policy is followed is not always consistent (see pages 39-41).
Setting goals for information and its management

At the time of our assessment, a Digital Strategy had been published in alpha form.\(^3\) The draft document set out a series of objectives, aspirations and goals, underpinned by key principles relating to technology, support and service provision and digital delivery.

We understand that there has been discussion within the House administrations about the need to embed information management in the Digital Strategy. This was included as a key objective in the Terms of Reference of the Information Management Authority (see page 34), and a number of interviewees stated that they thought this had been accomplished. We saw little evidence that this was the case.

The ‘business enabling’ aspiration does state that digital should support both Houses’ information management strategy. While this is a positive aim in itself, it is the sole reference to information management in the document and there is currently no information management strategy to link to, the previous strategy having lapsed in 2013. The production of a new strategy was included as a goal in the November 2015 Terms of Reference documentation for the Information Management Authority. We gained no assurance that work on this had begun since the governance body’s foundation.

The 2014 Parliamentary Information and Records Management policy includes a set of seven good-practice-enabling principles and outcomes that could go some way towards bridging this gap. These relate to the following areas:

- effective information management and ownership of information assets
- protecting information and sharing it responsibly
- producing accurate information and maintaining and disposing of information appropriately.

However, the principles are not specifically supported by an enabling plan and are not referenced in key documents such as the Archives business plan, the

\(^3\) The Digital Strategy: https://hackpad.com/A-digital-strategy-for-Parliament-OeyPfh3KPbe
Information and Records Management Service business plan, the 2016 IM Practitioners group action plan, or the draft Parliament Digital Strategy.

The House administrations are undergoing a period of change at the moment, with significant changes to the IT environment in particular likely to affect the way they manage, protect and exploit their information. Key among these are the projects to embed and gain benefit from the MS Office 365 environment and to introduce a replacement for SPIRE, which utilises Meridio software. Support for this is due to be withdrawn in February 2017 and the Meridio Replacement Project has been set up to find a new solution.

To provide a stronger framework for joint planning, the Digital Strategy should more explicitly reference IM, IA and information exploitation related outcomes. These would sit well under a number of the strategic aspirations that the document establishes. In particular, we recommend that there should be specific reference to the Meridio Replacement Project within strategy actions.

More detailed goals and outcomes to enable good IM in the new technology environment should then be positioned underneath the Digital Strategy or linked to it. See recommendation 1.

Enabling public access to information and supporting transparency and re-use

The House of Commons and the House of Lords are separate public authorities for the purposes of the Freedom of Information (FOI) Act 2000. The FOI performance of the House administrations does not fall within scope of the Ministry of Justice’s statistics on implementation of the FOI and Environmental Information Regulation (EIR) Acts and as such FOI arrangements were covered in light-touch form only by this IMA. We were pleased to note, however, the evident priority attached by senior staff to ensuring timely responses to FOI requests. We were also pleased to note the emphasis placed on enabling access to information by the parliament.uk website, with links to Transparency publications and to the Parliamentary Archives accessible through the main FOI pages.
We note that the Parliamentary Information and Records Management Policy is published on the parliamentary website in line with good practice principles set out in the S46 Code of Practice. Government departments are required to publish retention or ‘what to keep’ schedules, setting out their policies on what types of records to keep, and for how long, to provide greater transparency on decisions on retention and disposal.\(^4\) The House administrations have also published their Authorised Records Disposal Practice (ARDP). This is good practice.

Information published on the parliament.uk website is available for re-use via the Open Parliament Licence. This is equivalent to the Open Government Licence. We saw positive indications of a commitment to proactively publish information in areas that are subject to the most public interest and note that data.parliament has been set up on an open standards basis, enabling the publication of linked data and the provision of a SPARQL endpoint to enable data re-use. This is good practice.

### 1.2 Managing information as a valued asset

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

#### Defining and cataloguing information assets

An established process is in place for oversight of sensitive information assets, based around a template Register of Sensitive Information Assets that was drawn up in 2012. Registers of Sensitive Information Assets are updated at least annually as part of assurance processes. To supplement this, the House administrations have sought to identify their most sensitive information assets. This is good practice.

Registers of Sensitive Information Assets allow a basic range of context to be collected about each sensitive information asset under the categories ‘asset

\(^4\) This was recommended in Sir Alex Allan’s 2014 *Records Review* report: [www.gov.uk/government/publications/records-review-by-sir-alex-allan](http://www.gov.uk/government/publications/records-review-by-sir-alex-allan)
description’ and ‘security of asset’. We did not have the opportunity to review an example of a completed register, but one interviewee gave advice to ministers as an example of the type of sensitive information asset that they had logged. Underneath the main headings, subheadings are provided to capture key context such as protective marking, information asset owner, access controls and whether the format of the information asset is electronic or paper.

In addition, a separate Information Ownership Project has been set up under the Enabling Technology Programme to create and populate a series of new Information Asset Registers. Promotional material produced to publicise the Information Ownership Project states: ‘If we want to make the most effective use of our information, we need to know where it is and who is responsible for it.’ The project is positioned as ‘crucial ground work that allows us all to better understand and value information as a corporate asset’. This work was due to complete following our assessment.

The Information Ownership Project has created its own new template Information Asset Register. This differs from the existing Registers of Sensitive Information Asset and in our view provides a more straightforward and complete template that also has headings closer to those recommended by The National Archives. These cover key considerations such as purpose, storage location and disposal, the latter having been added to the template as a new criterion in 2015. The template Information Asset Register also provides brief pointers under each heading to guide those populating it. These ask questions such as ‘Who has access to the information? How is access controlled?’ This is good practice.

The Information Ownership Project has adopted the open and inclusive definition of an information asset promoted by Cabinet Office and The National Archives. This is particularly pleasing to note as, unlike government departments, there is no requirement for House administrations to adhere to guidance published under the Security Policy Framework. Documents we reviewed suggest the House administrations have followed through on their definition in practice and have not

---

restricted their information asset governance approach to either IT systems or to personal information or to significant datasets, as we have seen in some government departments. The definition appears to have been well interpreted by staff, with information assets catalogued on the basis of broad related groupings of information. This is good practice.

The inclusive basis on which staff are expected to populate Information Asset Registers means that they offer considerable potential utility as a management tool. We saw positive indications that the work to create and populate Information Asset Registers had been pursued with a view to mitigating risks relating to a lack of knowledge of information held. We were told that workshops have been held that encouraged teams to think about how information flowed between them. The creation of Information Asset Registers has also reportedly provided a spur for some teams to rethink the sensitivity of their information assets. This is good practice.

While we found recognition of the local benefit obtained from the process of creating an Information Asset Register, we did find some lack of clarity among interviewees about the overall purpose of the project and its status. This may, in part, be due to resource related delays mentioned in the Information Ownership Project highlight documents that were supplied to us. One member of staff said:

‘It felt like duplication as there is already a sensitive asset register. It was sold OK when I asked, though, as something looking for synergies and overlaps. But where has it gone? I fed into the first version a year ago … and have no idea where it went.’

The completion of the project and transfer of this work and proposed ownership by the Information and Records Management Service (IRMS) offers an opportunity to re-energise this work, increase its profile and promote its value to the business to ensure necessary levels of buy-in. At the same time, we recommend that the House administrations review the current siloed approaches to cataloguing information and data assets with a view to establishing a consistent approach and minimising duplication. At a minimum, the House administrations should ensure that the same
context is collected for what they term sensitive information assets as is enabled by the Information Asset Register for information assets. This could, for example, be achieved by adopting a single template register. See recommendation 2.

**Ownership of information assets**

The House administrations have undertaken training offered by The National Archives in Information Assurance and cyber-security. At the time of the IMA, reporting requirements had not been defined in relation to Information Asset Registers and we noted told that there was some inconsistency in the level at which the IAO role was established.

We were told that there had been a recent push to clarify the role of the IAO, but saw limited evidence that it had a high profile or was widely recognised, or that the value it offers to the House administrations was generally understood. We recommend that the role is formally reviewed as part of work to simplify and consolidate the current separate approaches to defining and managing its information assets. Once expectations of the role are fully defined, clear guidance should be provided to staff. See recommendation 2.
2 Information and supporting technology

2.1 The technology environment

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

Enabling information management
SPIRE supports the lifecycle management of digital information and records and meets key requirements of the Section 46 Code of Practice for storage of records. This includes enabling routine records management processes to take place. We commend the House administrations for the effort invested in maintaining and improving SPIRE since its introduction in 2012-13, but note that interviewees expressed mixed opinions about the system.

Although few strongly positive endorsements were offered, a number of staff did indicate that the system provided them with a straightforward environment for file creation. One, for example, suggested that SPIRE ‘works about as well as a system like that can be expected to’, while another suggested, ‘SPIRE gets a lot of stick, but it isn’t the worst thing I’ve ever seen.’ A third said ‘I don’t really like the SPIRE tech… but people feel well supported in actually using it.’

By contrast, a number of staff did provide strongly negative opinions on SPIRE. A range of factors appeared to have helped undermine user buy-in to the system. There was a common perception that SPIRE was slow and old-fashioned, with staff suggesting that the ‘world had moved on’ and that it was ‘old technology’ with an ‘unhelpful’ interface. One interviewee said, ‘It is extremely slow and doesn't interact intelligently with the other computer systems.’ In addition to a straightforward dislike of the system, other issues referenced by interviewees from both administrations included a lack of confidence in it and an inability to store certain types of documents. Remote access was highlighted as a particular problem. One interviewee for example said, ‘SPIRE is clunky and has downtime, and you cannot
access it through the Cloud… It doesn’t reflect how we need to work and need to access information on the move.’

In addition to SPIRE, a range of alternative corporate locations are available to staff for the storage of information. OneDrive and SharePoint Online have been rolled out to a limited number of users, the latter as a collaboration tool with its governance jointly owned by the Parliamentary Digital Service (PDS) and the Information and Records Management Service (IRMS). A number of staff still have access to personal and shared drives.

None of these environments in themselves enable information life cycles to be managed corporately in accordance with the Authorised Records Disposal Practice (ARDP). As a result, information held in these areas may be deleted by staff before it should be, may be more or less accessible than it needs to be, may lack required audit trails, or may be held for longer than it needs to be or should be. As is recognised in the current House of Commons SIRO risk register (see page 33), this may raise risks related to efficiency and effectiveness. It may also raise risks related to the ability to ensure the security of information, and to comply with the Data Protection Act.

The situation is compounded by the limited control that is currently exercised over the size of email accounts. The House administrations have removed a potential technical barrier to corporate storage of email by enabling easy transfer of emails to SPIRE via drag-and-drop functionality. This was recognised as a positive feature of the system by several interviewees. Despite this, it is clear that a cultural barrier to corporate storage of emails remains. A number of interviewees told us they were holding large volumes in their email accounts. One said: ‘I have about 5,000 emails in my inbox. My boss is worse than me. I’ve tried to manage them but have not been successful. I don’t store emails in SPIRE – I’ve got an expanded inbox so never get the message about running about of space.’ Another said: ‘I keep my emails in my inbox – PDS are always telling me I have got too many in there.’ A third said: ‘I’ve got thousands and thousands – it’s my main filing system, sadly. I’ve probably got every email I’ve ever received.’
The variety of potential repositories available and the varying degrees of oversight to which they are subject make the risks raised more significant. Of added concern is the storage of information in non-corporate locations. This includes both personal devices and applications and systems acquired independently without going through required the centralised procurement and accreditation processes (see page 29).

Although the House administrations state that many staff use SPIRE for both filing and for working documents, not all of the staff we spoke to did as discussed below (see pages 39-41). We recognise that the requirement for staff to move records to SPIRE is a mitigating action for the risk that information with value is not captured. However, in our view, the core benefit that SPIRE has offered the House administrations has been undermined by the provision of a wider IT environment that does not enable information and records management outcomes.

This suggests a lack of joint planning for IT and information management in the past. PDS and KIM colleagues are now investing considerable effort into trying to mitigate the risks that this situation has created. This makes it all the more important that a joint strategy is pursued in the future. This should include a strand relating to improving culture in relation to email and personal storage of information. The staged programme put in place recently by IMA programme member the Welsh Government, with support from senior management, provides a good-practice example of how this kind of issue can be tackled. See recommendation 1 and 4.

**Finding, accessing and protecting information**

Among those currently working within the corporate MS Office 365 environment, we found broadly positive views about the opportunities it offers for sharing and collaborating on documents, mobile working and working across different locations.

In a number of cases the benefits noted, such as the ability to share links through One Drive and SharePoint, should in theory have been offered by SPIRE. In the case of the ability to set individual permissions, which one interviewee saw as a key benefit of SharePoint, this circumvented controls built into SPIRE.
SPIRE users are encouraged to set permissions at a group level and the system allows IRMS staff to review and audit these and check they are applied correctly and as openly as possible. In the one case where an interviewee indicated that help had been sought from IRMS, it was clear that a number of longstanding issues had been resolved and an end had been put to ‘endless complaints about not being able to access certain links’. Where group permissions within SPIRE are not set up correctly, the standard four-hour lapse in amending them may be an issue for staff working to tight deadlines, together with the fact that amendments have to be done through Record Officers rather than by staff themselves. One interviewee also noted that the process was not particularly intuitive and could go wrong, ‘so people can sometimes think they are giving access when they are not’.

Staff using SPIRE can perform searches by content as well as document titles, although this functionality has been impacted by a number of underlying problems with the system’s search index. An overall summary of the situation was provided by one senior member of staff who stated: ‘I think SPIRE has been a really good tool, but it hasn’t got [everything] that should be in it and it is sometimes difficult to retrieve what you need … If you ask me to find anything in SPIRE, I couldn't.’ Two staff described it as ‘a one-way filing system’: one said, ‘You put things in there and you never find them again.’

In preference to utilising the search function, some interviewees stated that they were either relying on their Record Officers to find information for them or on browsing the file plan. The ease of the latter will depend on familiarity with filing structures, the adoption of logical structures and application of helpful naming conventions. IRMS has been working to flatten the file plan: its depth and complexity in some areas may be a barrier to the easy location of information. For example, one interviewee noted: ‘In my last role there were only a couple of places that information could be saved. In my current role, neither search function nor logic helps.’

Incorrectly set permissions and difficulties finding information within SPIRE are likely to be contributing to
• staff holding information they need to access outside SPIRE
• the use of workarounds when staff need to exchange information, raising risks relating to version control
• limitation of the degree to which staff are willing to search for information and knowledge outside their own immediate working area in SPIRE.

Where information with value is held in locations not subject to corporate oversight and control, the House administrations are entirely dependent on local knowledge and support to find it. While staff may still be able to do this in the short term and at a local level, the dispersal of information across a range of systems and platforms will make it harder to do so from an organisational point of view and may do so particularly where older information is concerned.

The current technology environment presents a number of barriers to the quick and easy retrieval of information, which is a key requirement of records systems set out in the Section 46 Code of Practice. This includes SPIRE itself. The House administrations should ensure that the Meridio Replacement Project and MS Office 365 programme work together to address risks flagged in sections 2.1 and 2.2 relating to records storage and retrieval. For example, the ability to control and monitor permissions must be balanced by ease of use and the effort that has to be invested to ensure they are administered correctly. See recommendation 3.

Once the corporate MS Office 365 environment is rolled out more widely and the Meridio replacement is in place, barriers such as those that currently prevent remote access to SPIRE will be removed. The House administrations should then investigate opportunities for imposing proportionate technical restrictions on alternative repositories to ensure that large volumes of information cannot be retained there. This must be accompanied by a clear, promoted policy line. See recommendation 4.
2.2 The continuity of digital information

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

Oversight of information and digital continuity planning

Interviewees indicated that the House administrations hold a total of somewhere between 200 and 300 TB of unstructured information and data in Line of Business systems, with information distributed across a number of repositories as noted above. Interviewees indicated that the House administrations are already experiencing some digital continuity issues in relation to the completeness and ability to trust some data in line of business systems.

The House administrations do not currently know the volume of information that is held by administration staff in shared and personal drives. In addition to information held outside shared corporate repositories in Microsoft Outlook, further volumes are held in .pst format: these represent a higher level of risk. This is both from a security point of view, in light of their portability, and from a digital continuity point of view, as they are held outside corporate spaces and are particularly vulnerable to file corruption.

Interviewees indicated that it has historically been a challenge to understand what systems are in use and what information is held in each location. We saw little evidence that PDS and IRMS have yet developed a shared, detailed understanding of what information the House administrations hold.

The House administrations have included use of The National Archives’ file profiling tool DROID in the scope of their programme of health checks. IRMS has carried out some discovery work in relation to the shared drives using this tool. We are pleased to note a commitment to limit the provision of shared drives in the new technology environment and a commitment to review their contents and migrate information of value. The House administrations should consider the use of DROID to support this work to help understand what information is held in them. The Information
Ownership Project has the potential to complement this work through the provision of a business-led summary of information assets held that covers all repositories. Work to further roll out and realise benefits from MS Office 365 and the Meridio Replacement Project should also make use of this resource. See recommendation 3.

Positive steps to identify key digital continuity priorities have been taken. A workshop was held in early 2015 between IT and colleagues from the Parliamentary Archives, with a view to identifying points in the IT Lifecycle model where digital continuity could be embedded. This work has been on hold since the formation of PDS and changes in key personnel. We recommend that it should be restarted and that digital continuity planning for the new IT environment should be embedded within the Digital Strategy. See recommendation 1.

**IT change**

The House administrations have recently focused on improving governance around the IT procurement and accreditation processes to clarify and document procedures and ensure the right people are linked in. The approach is bicameral and centralised. It is also flexible, with three different accreditation pathways available, depending on the significance of the solution that is proposed. For the most significant of these, interviewees indicated that a full process of checks and balances was in place with a requirement to provide a statement to the Cyber Authority.

We were pleased to note that the accreditation and procurement process covers disposal as well as information security considerations. While this represents a good start, lessons should be learned from the application of information and records management controls within the current technology environment.

More should be done to ensure information and records management requirements such as retention are consistently factored into the design and implementation of new systems in the future. Doing this would support the objective set out in the Parliamentary Information and Records Management Policy that information and records management requirements must be integrated with technology planning and
strategy. It would also help support the Digital Strategy’s ‘secure technology that works’, ‘effective’ and ‘efficient, reducing cost’ aspirations, acting as an enabler for the more joined-up strategic approach for IT and IM/RM that this report recommends. A formal link should be established between the procurement and information asset governance processes to ensure that any new information assets created can be identified and logged. IRMS should also be identified as a key stakeholder rather than only being consulted in relation to future disposal requirements for sensitive information. See recommendation 5.

A number of interviewees highlighted concerns about consistency of practices and the ability of staff to procure systems without engaging with the corporate IT procurement and accreditation process. One noted a lack of apparent reprimand in cases when this happened and suggested that a ‘single mandate’ should be in place, while another suggested that the solution lay in more effectively meeting user needs. While a number of our interviewees had or were engaging with the corporate process, the validity of these concerns was borne out by one member of staff who said:

‘I refuse to use Parliamentary technology as it is too locked down and half the functionality is shut off. I would rather pay out of my own pocket for kit… [People are] so frustrated by it all that they just do their own thing.’

This kind of behaviour represents a significant source of risk for the House administrations, with a range of impacts in terms of their ability to effectively manage, protect and exploit information. It must be addressed as a priority. See recommendation 5.

The Meridio Replacement project
The name of the Meridio replacement project was chosen to emphasise a move away from the current Meridio software rather than the idea of corporate records storage that SPIRE was meant to embody. The business case for the Meridio Replacement project was developed during 2015 with input obtained through a series of 1:1 interviews with Records Officers and focus groups with Records
Officers and staff. A staff survey was also conducted to give feedback on the present system and find out what they would like to be able to do that they cannot with existing technology. **This is good practice.**

At the time of the IMA the business case was still under development. Consideration has been given to a like-for-like replacement using alternative traditional EDRMs software, to procurement of ‘out of the box’ SharePoint Online and to procurement of SharePoint Online with records management and email integration plug-ins. We emphasise that SharePoint by itself does not currently deliver records management outcomes. Plug-ins are required to enable these. **See recommendation 3.**

The Meridio Replacement project is running alongside work to fully roll out and realise benefits from MS Office 365. This is larger in scope due to coverage of members as well as staff of the two administrations. We gained a good level of assurance that PDS and IRMS colleagues are working together on both projects, with recognition of the need to work together to co-design SharePoint architecture. We also gained a good level of assurance that a consensus view is being reached on what the Meridio replacement needs to deliver and that benefits from SPIRE are being factored into the project. However, we note that the relationship between the two had not been fully formalised at the time of the IMA. This needs to be done as a priority. **See recommendation 3.**

Implementation, roll-out and embedding work must be given at least as much weight as procurement itself. Continued priority needs to be given to ensuring that user needs are factored into the design and architecture of the new system. Particular consideration needs to be given to culture to encourage buy-in and support for the new system. This is important because:

- there is potential for erosion of good practice ahead of the new system’s introduction
- the Meridio replacement will differ to the current implementation of SharePoint, which itself reportedly varies from team to team
- a percentage of staff are very familiar with SPIRE.
The House administrations should build on lessons learned from previous roll-outs. Based on the statements of interviewees, the integrated approach adopted for the launch of SPIRE contrasts positively with that adopted for the partial roll-out of SharePoint in 2014-15, which left some staff unclear how the new system should be used. See recommendation 4.
3 Information risk, governance and oversight

3.1 Recognising information risks

<table>
<thead>
<tr>
<th>Goal: The organisation defines and manages information risks to minimise threats and maximise opportunities.</th>
</tr>
</thead>
</table>

**Documenting and defining information risks**

Cyber-security risk receives Board-level scrutiny as one of the key security risks for the House administrations. Two high-level risks relating to cyber espionage and cyber sabotage have been defined. These are owned by the Parliamentary Security Director.

Information and records management related risks have been defined by both House administrations. Information and records management related risk is visible to the SIRO of both administrations. **This is good practice.** However, risks are owned, logged and overseen in a different way by the two administrations as discussed below.⁶

Once digital continuity principles have been defined and incorporated into the Digital Strategy, the two administrations should document the risks they face in relation to the ability to find, open, understand, work with and trust information over time and through change. **See recommendation 1.**

**Implementing an information risk management approach**

Across both House administrations we found a good level of informal awareness of risks relating to knowledge loss, information security and information integrity. We are also aware that the House administrations have conducted a number of initiatives aimed at mitigating cyber-security related risks from a technical and cultural point of view, including penetration testing and awareness campaigns on topics such as phishing emails. **This is good practice.**

---

⁶ We viewed hard-copy printouts of risk descriptions in the course of a briefing meeting in the run-up to the IMA, but were not permitted to take these away or provided with copies. Our findings are based on notes made at the time rather than a detailed, desk-based review.
In the House of Commons, information and records management related risk is one of five high-level risks with an administration-wide impact that is recorded on the SIRO risk register. The risk was under review at the time of our assessment. The risk description focuses on the threat of premature destruction of information, recognising potential cultural, governance and IT related causes and potentially negative impacts on efficiency and effectiveness.

In the House of Lords, risk relating to information and records management and FOI has been delegated down to each of the administration’s departments to manage. As a consequence, most departments of the House of Lords have identified risks related to their own performance, which were defined in simple terms such as ‘poor records management’ or ‘data loss’. The risk defined by the Parliamentary Archives, however, highlights strategic level causes and threats and administration-wide impacts in relation to decision-making, litigation and reputation. This has been logged at the same level as the other departmental risks rather than at a level above them. We also note that the Parliamentary Archives have not contributed a risk of the kind defined by other departments related to their own standards of information and records management. This suggests that the delegation of information and records management risk has not been carried out consistently.

While it is appropriate to delegate responsibility for adherence to standards to individual departments, other risk factors that apply across the whole administration do not belong at this level. These should be captured and logged at a higher level within the risk management framework.

In our view, both House administrations may currently be overlooking causes and threats that could have an impact on them because they have adopted separate approaches. The fact that both Houses are separate legal entities needs to be balanced with the fact that the results of poor performance in this area are likely to be comparable. The requirements of the Information and Records Management Policy apply to both House administrations equally, some information is joint and the core records of both administrations – whose staff use the same IT systems to
conduct their business – are ultimately due to end up in the same Parliamentary Archives.

We recommend that the House administrations review their approach to information risk once information and records management objectives have been fully embedded within the Digital Strategy. There would be benefit in adopting a more joined-up approach to oversight of information and records management related risk, as has been achieved for cyber-security related risk. See recommendation 1.

3.2 Establishing control

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

Governance structures

The Information Management Authority was established to provide a means of facilitating strategic co-ordination on information management related issues across Parliament. It was set up on the same principles as the existing Cyber Authority. Members of both bodies are board level and membership of the two authorities overlaps. Terms of Reference for the Information Management Authority were finalised in November 2015 and position it as a body with a strategic focus and a remit concerned with oversight, co-ordination and driving targeted improvement in governance and policy.

The Terms of Reference for the Information Management Authority state that the body’s powers are derived from the responsibilities of its members, as delegated by the two Clerks. It is supported by two bodies: an information management practitioners’ steering group (made up of IM professionals), and an information management forum with a consultative function (made up of senior business representatives from across Parliament). While this arrangement provides a sound foundation for the board, we note that work on key priorities, such as agreeing an Information Management Strategy, had not begun at the time of the IMA. In addition,
although views expressed about the aims of the Information Management Authority were generally positive, a number of interviewees raised questions about it. These related to its impact and focus, together with the extent to which it is positioned to act as a decision-making body and the extent to which its remit overlaps with that of the Cyber Authority. In view of this and of the recent governance changes noted below, we recommend that the House administrations review the provision of current information-related boards. In doing so, the House administrations should ensure information and records management gains a comparable level of senior oversight and input to that which is intended now.

This is important because of the distributed ownership of different aspects of information governance within the House administrations and because of the common factors noted in section 3.1 above as drivers for a more joined-up approach for information management risk (see p.29). There may be benefit in establishing a single strategic board, either by itself or one that is supported by other boards focusing on specific issues such as information assurance, cyber-security and information and records management. In particular, this should identify clear responsibility for work needed to drive, improve and maintain the culture that will ensure full benefit is obtained from the new technology environment. See recommendation 6.

Such considerations are particularly important in view of the departure of senior staff and champions in the months after the IMA. We regard an active senior champion as a crucial enabler for a supportive culture. The House administrations should define how information and records management will be championed and owned at Board level. See recommendation 6.

Supporting the business
The Parliamentary Archives exist as a shared service rather than as a joint department of the House administrations. It delivers the following core activities: information and records management by the Information and Records Management Service (IRMS), selection and acquisition, preservation, public information, and access and outreach activities. At the time of the IMA the Parliamentary Archives
were based in the House of Lords’ Department of Information Services. Following the departure of the Director of Information Services in March 2016, it moved under the SIRO and Reading Clerk. At the time of the IMA, the sponsor in the House of Commons was the SIRO and Director General of HR and Change, who is due to leave Parliament in autumn 2016. Following the IMA the Director of Research and Information became the House of Commons’ client. At the time of writing this report, the location of SIRO responsibilities had not yet been decided.

The Parliamentary Archives’ Memorandum of Understanding and Statement of Services to be Delivered establishes the basis for the shared service to be delivered in each financial year, setting out priority areas for IRMS and other archives staff, together with key staffing and governance requirements. The Memorandum of Understanding for 2016-17 was in draft at the time of the IMA.

IRMS has produced a Customer Service Charter that was endorsed by the Business Management Group in the House of Commons and Business Planning Group in the House of Lords in July 2014. This sets expectations for the team in terms of service standards and for the business in relation to compliance with policy. **This is good practice.** The document identifies four main headings under which the team’s work falls:

- advice and consultancy
- information risk assurance
- building capacity
- customer and system support.

The Customer Charter and these four areas are cross-referenced in the Memorandum of Understanding.

We note that there is a commitment in the Parliamentary Archives 2017-18 business plan to revisit and update the customer charter. We recommend that a short-term update of the charter is done now to clarify priorities for the coming year. A new
version should be issued to tie in with the launch of the new IT system. See recommendation 7.

The Parliamentary Archives’ business plan is aligned to House of Commons and House of Lords strategic objectives for the period. This is good practice. It establishes strategic deliverables for IRMS over and above the priority areas set out in the customer charter. A spot check of the IRMS business plan for 2015-16 indicates that it covers off key priorities under each of the four headings in the charter. We recommend that any further team plans explicitly reference the Parliamentary Archives’ business plan priorities and Customer Service Charter headings. We also recommend that the relationship is clearly defined between IRMS and the Parliamentary Archives’ business plan documentation and any future action plans produced by bodies such as the Information Practitioners’ Group. See recommendation 7.

Support networks
There is currently a network of around 220 Record Officers for a total of circa 2500 staff across the two administrations. There were a small number of unfilled Record Officer roles at the time of the IMA. The Parliamentary Information and Records Management Policy establishes Record Officers as one of the records management related roles that heads of department or office are responsible for assigning. This is good practice. It states that the role should act as the link between the business and IRMS. It is left to teams to decide whether Record Officer responsibilities need to be included in staff objectives. In our view, this should be standard practice.

For many Records Officers, a majority of their role is SPIRE focussed, and all teams have to have a Record Officer in place if they want to access SPIRE. The core responsibilities of Record Officers are:

- liaising with the IRMS to ensure compliance with policies and procedures in their area
- providing advice to staff on the local application of policy and practice
• training new staff on local information and records management practices and procedures
• reporting to the head of their business unit areas of non-compliance and other issues as they arise.

The Record Officer role appeared to be delivering benefit in a number of teams we spoke to, with staff noting that Record Officers assisted with basic records management queries including the creation of template folders within SPIRE. The process by which Record Officers can request these appears straightforward.

The IRMS strategy and forward plan for 2015-16 includes a specific action to proactively support the development of records officer capability, awareness and skill. We saw evidence that they are actively working to do this through a range of means, including an annual general meeting, a quarterly newsletter, targeted emails and an annual records officer desk calendar. **This is good practice.** The latter provides a useful means of communicating helpful information and reminders of key requirements for the role. The pages at the front of the calendar set out the main elements of the customer service charter and the ‘what to keep and where’ guidance referenced below (see page 39). The page for each month includes a photograph from the Parliamentary Archives and a series of reminders on routine and date-sensitive activities that need to be undertaken. These range from setting retention trigger dates to reminding teams to review and clear out redundant emails. At the back of the calendar, there is an overview of how to unlock a document in SPIRE, how to change a Record Officer password and the process to follow in relation to a change in Record Officer.

The Record Officer and lead Record Officer roles should be reviewed ahead of the introduction of the new technology environment. The review should be added to the Parliamentary Archives’ business plan for 2016-17 and 2017-18. Both offer considerable potential ongoing value. **See recommendation 7.**
3.3 Providing direction

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

Knowledge and Information management policy and guidance
The 2014 Parliamentary Information and Records Management Policy establishes information as a valued corporate and public asset. It meets key recommendations for policy documentation as set out in the Section 46 Code of Practice. It has, for example, been endorsed at a senior level, with approval from the Clerk of the Parliaments and Clerk of the House, and outlines key roles and responsibilities. It builds on the recommendation to specify the responsibility of individuals to document their work by also setting out the specific responsibilities of line managers and heads of departments and offices. The latter are broadly responsible for strategic oversight and ownership of related risk, while the former are responsible for ensuring staff are aware of their responsibilities and have sufficient time available to them. This is good practice.

Knowing what to keep and where
A range of guidance is provided to staff to help them interpret the Parliamentary Information and Records Management Policy and ARDP. Individual documents have been developed, setting out how specific systems should be used. The documents we reviewed provided a consistent steer that information with value should be stored in SPIRE.

The ‘Where to Store Information’ quick reference card is particularly noteworthy for its straightforward summary on when to use SPIRE and when to use personal spaces, shared drives and SharePoint. It includes a statement that staff are themselves responsible for reviewing information held outside SPIRE and either deleting it in line with the ARDP or moving it to SPIRE. It also emphasises that staff have a specific responsibility to review the contents of personal and shared drives and SharePoint, and to either delete information in line with the ARDP or move it to SPIRE.
The staff we spoke to were generally clear on the role of SPIRE, with one interviewee commenting that using it 'is a minimum requirement for things you don’t want to lose'. Another, who noted the system’s limitations, said that all final documentation and important information went into SPIRE with their files serving as their 'official record'. It is clear, however, that levels of compliance vary between individuals and teams.

A number of interviewees gave their view that staff in some cases are simply choosing not to follow policy. One said: ‘Policies on OneNote and OneDrive are fine and communicated – and ignored.’ Another gave their view that the availability of repositories, such as generous email inboxes, undermines policy: ‘Corporately the organisation is saying, there is this room, don’t go in there and use it – but we are going to leave it unlocked for you.’ A failure to meet user needs was identified as a reason to adopt workarounds and a number also highlighted staff awareness that SPIRE was being replaced as a factor.

While the guidance we saw on which systems to use and which processes to follow was clear and straightforward, we note that it does not reflect the corporate line expressed in the 2014 Parliamentary Information and Records Management Policy. This states that information held in other corporate repositories outside SPIRE should either be moved to SPIRE or printed to paper. It makes no mention of the need to review information in line with the ARDP or of the requirement to delete information that has no value.

With the transition to the new technology environment in mind, the House administrations should revisit their policy for the coming year to ensure a clear and appropriate message is given to staff for the period before the introduction of the Meridio replacement. This should be done in addition to the scheduled 2017 review of policy that is included in the Parliamentary Archives business plan for 2016-17 and 2017-18. The House administrations should take the opportunity to make other updates to reflect the current organisational structure. See recommendation 7.
In contrast to those interviewees who felt staff were choosing not to follow policy, a number of interviewees felt that key messages on how information should be managed are absent or are being missed or misunderstood. This applies to issues such as which emails to capture and to capturing decisions taken in meetings and by phone. It also applies to the way in which systems should be used, with questions raised by staff from both administrations. One noted:

‘Each team is largely a world of its own. [The volume of] correspondence and documents is increasing and quite a lot of information is held informally, a bit like an iceberg. Opinion about what needs to be managed where is quite varied. Tech was bought in to help manage that, but there is no clear idea of what goes into what system at what point. Some use OneNote, some use SharePoint. Some feel they don’t need to use SPIRE as they have SharePoint. It is confusing … and compliance is decreasing.’

This was echoed by a second member of staff, who said:

‘There has now been a big push to use SharePoint and it is a bit of a muddle what goes where. There is an expectation that things should go to SPIRE at the end of the year, but there needs to be a clear message on where to put things.’

A third also said:

‘There is no clear mandate to use one system, so information is quite distributed. Areas all take their own approach and there is no consistency.’

Once policy is clarified it must be actively promoted with senior support and a clear mandate by heads of department and line managers as well as Record Officers. See Recommendation 4.
Providing training

All new staff are required to undertake SPIRE training and we gained assurance that an active programme of training courses is also in place for Record Officers. This is good practice. Record Officers are expected to sign a code of practice when they have their mandatory introductory training. A total of 64 Record Officers undertook this in 2015-16 across 15 sessions. Additional access in SPIRE and disposal in SPIRE training is also provided, with nine sessions of the former and 22 sessions of the latter held in 2015-16.

IRMS has developed a new e-learning package for both House administrations that had just been launched at the time of the IMA. This uses real scenarios, covering the role of information management, basic requirements for staff, the disposal process and function of IRMS. This is good practice. In addition, a data protection related piece of e-learning has been launched for House of Commons staff and members. See recommendation 7.

At the time of the IMA the House of Commons induction process was under review. This has since been relaunched and we are pleased to note that the records management e-learning module has now been made mandatory for all new starters in both House administrations.

3.4 Measuring impact

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

Measuring compliance with policy

The Section 46 Code of Practice recommends that organisations should indicate how compliance with corporate policy and supporting standards, procedures and guidance will be monitored. The Parliamentary Information and Records Management Policy does not provide specifics but states that the Parliamentary Archives have overall responsibility for this, and that work will be carried out by
IRMS. The IRMS Customer Service Charter includes compliance monitoring activities among the Information Risk Assurance activities conducted by the team. It notes that the team will assess compliance ‘to monitor whether information that ought to be kept can be found, and information no longer needed is disposed of according to policy’.

IRMS and the SPIRE benefits realisation team both report a range of performance data relating to training, engagement and SPIRE usage on a quarterly and monthly basis respectively. In the House of Lords, performance criteria have been identified for information and records management, consisting of SPIRE usage, folders scheduled for and overdue for disposal, and resolution of SPIRE support calls.

At the time of the IMA, IRMS was also conducting a programme of health checks in the House of Commons and the Parliamentary Digital Service (PDS) following a pilot conducted in the House of Lords earlier that year. These focus on the following four areas:

- where and how information is stored (for example, in which systems)
- structure and organisation of information
- retention of legacy information and disposal in accordance with the Authorised Records Disposal Practice
- management of emails.

Conclusions are drawn from face-to-face interviews with Record Officers and other relevant members of staff, and from statistics on systems usage. This range of sources allows IRMS to gain qualitative and quantitative insights into culture and performance. We were told that the range of sources used could, for example, reveal whether apparently good engagement with SPIRE is down to a team-wide ethic or to the action of a few team members. By looking at document types stored, IRMS could also highlight where a relatively small volume of emails were being stored, suggesting that key context was not being captured. This is good practice.
Health checks result in a rating for each heading and advice on how to improve capability. They are positioned to encourage teams to interact with IRMS and engage with the training they provide. They are also used as an opportunity to check whether permissions are still correct. **This is good practice.**

We note that the tone of health checks is collaborative rather than directive, with outcomes being suggestions rather than recommendations and the lowest score being ‘advice given for improvements’. We also note that, when the plan to conduct health checks in the House of Commons and PDS was presented to Management Group in October 2015, they were badged as a ‘light-touch’ exercise rather than an audit of compliance with policy. In a paper drawn up for the Information Management Authority in January 2016, they were identified as the mechanism by which the Customer Service Charter commitment to monitor performance will be delivered. This should be clarified. In addition, we recommend that future health checks and any other monitoring activities conducted by IRMS are directed towards the line manager and heads of office/department roles that are identified in the Parliamentary Information and Records Management Policy (see page 39). By following through in this way, line managers and senior staff will be able to see whether they are meeting their obligations, how their staff are performing and where they need to improve. **See recommendation 4.**
4 Records, review and transfer

4.1 Oversight of records and selection

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

The role of Departmental Records Officer (DRO) is a recommended position within government organisations that was first established in 1954. The role should lead on compliance with the Public Records Act and maintenance of the statutory relationship with The National Archives and the Advisory Council on National Records and Archives. The House administrations are not public records bodies and therefore lack these legal drivers, but the Head of the Information and Records Management Service (IRMS) fulfils a comparable function in view of the team’s ownership of policy and practices for the end-to-end management of information.

The close involvement of the Head of IRMS and the IRMS team in the Meridio Replacement project shows that the role is currently well connected. In particular, we noted a good working relationship between the Head of IRMS and the SIROs of both administrations. The National Archives’ guidance on the DRO role recommends clear lines of reporting to the SIRO. In view of current governance changes and changes in senior personnel, there may be benefit in formally defining the relationship between key information governance related roles including the Head of IRMS. See recommendation 7.

Oversight, control and use of records

IRMS has full oversight of information stored in SPIRE. As noted elsewhere, the team has less oversight of information held outside the system, but has the opportunity to address this through the move to MS Office 365, the Meridio Replacement project and the creation of Information Asset Registers across both House administrations. The creation of Information Asset Registers led to the creation of new disposal schedules within the ARDP. This is good practice.
Health checks are used by IRMS to ask whether any undeclared hard copy records are being held locally. While processes for the archival storage of records are out of scope for this report, the fact that separate archives exist within the Parliamentary Estates Department is of interest. The department has an obvious business need to access and consult these records, which provides a reason for them to be held locally. However, unlike records within the main archives, we note that they will not be stored to British Standard for Archival Storage PD 5454 standards. We recommend that the relationship between the two is reviewed with a view to balancing the need to maintain appropriate and secure conditions for document storage and to enable business access to records worthy of permanent preservation. **See recommendation 8.**

**Appraisal and selection**

The 2012 Parliamentary Archives Collections and Acquisition Policy provides a statement of collecting policy for internal and external records, including in relation to repatriation of records, private papers of significant Parliamentary officials and to architectural and photographic records. It sets out exceptions, including public records, and records that are not practical to store or otherwise too damaged or incomplete to offer value. The policy establishes 11 historical selection themes and also sets out the means of acquisition and basis for access. The ARDP sits beneath this and defines retention policy for specific record types, ensuring staff have guidance on when and how to dispose of information in all formats and system.

Appraisal is conducted by Parliamentary Archives staff in accordance with these appraisal criteria, and guidance is provided on recording appraisal decisions in an Appraisal Decision Form; this includes a list of standard appraisal phrases to aid decision making. There is an expectation that Record Officers will be involved in sift and appraisal processes: we were told that, where possible, blanket decisions are taken in relation to the selection of particular types of record. **This is good practice.**
4.2 Implementing disposal decisions

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

Triggers for disposal

Within SPIRE, the Classification Scheme for Parliamentary Records allows disposal and access criteria to be applied to the file plan via keywords at different levels with criteria inherited from above. Where consultation with the business on how long to keep records identifies a new disposal schedule, this will feed into the ARDP with updates made to the file plan and search as necessary.

Work has been undertaken to clean-up SPIRE and to identify unused folders within the file structure. In addition, a manual process is in place to facilitate disposal of records in practice. This piloted in October 2014. A total of 771 folders had been disposed of by the end of the financial year. Record Officers are able to run reports identifying disposal due over the coming year, with many triggers for disposal based on the end of sessions or of the financial or calendar year. Disposal decisions need to be authorised by the relevant IAO, providing a robust link into the information asset governance process. This is good practice.

While we saw some indication that there may still be apprehension about approving deletion of records, it was clear that routine disposal processes are taking place in a number of areas. The House administrations are some way ahead of a majority of the government departments we have assessed, particularly in view of the fact that the print-to-paper policy only ended officially in 2012.

The House administrations are aiming broadly to move only information with value out of the existing shared drives when the Meridio replacement is introduced. They have also sought advice from a technical point of view on the migration of information from SPIRE as a component of the Meridio Replacement project. The following have been identified as factors that will put Meridio in the best possible state beforehand:
• removing redundant access groups, and ensuring required groups are up-to-date
• ensuring that there is no orphaned information in the system
• removing unused, redundant or empty parts of the SPIRE file plan
• supporting teams to increase disposal activity, ensuring that information which should be destroyed is deleted, and information of long-term value is exported to the Digital Preservation system.

There is an expectation that this work will continue through to the roll-out of the Meridio replacement and will form part of the preparations for individual teams.

**Sensitivity review**
The House administrations are currently trialling approaches for the sensitivity review of digital records using open source BitCurator tools.

Existing processes for the sensitivity review of records are business led and differ from those adopted within government departments. All boxes containing hard-copy records should come into the Parliamentary Archives with a form detailing sensitivities or closure requirements. The form is sense checked and the records are examined for any obvious sensitivity. Staff have freedom to select their own security or data protection related closure periods. Space is provided for staff to add context on the reason for closure decisions. However, we note that this is not a formal requirement and no guidance for staff was in place at the time of the IMA. This raises the risk that staff may be selecting inappropriate timescales and that inconsistent decisions are being applied. We recommend that guidance on how to select and apply closure periods is produced. The House Administrations should also define how this will be tested when records are received by the Parliamentary Archives. See recommendation 8.

**Transfer and planning**
A combination of a relatively fixed set of functions and activities (in comparison to government departments), good use of retention scheduling and timely disposal of
records means that the House administrations have an effective and efficient process in place for the transfer of paper records to the Parliamentary Archives.

The House administrations also have their own digital repository, based on Preservica digital preservation software. This has been operational since 2014 and allows ingest workflows from a variety of different sources including data.parliament.

A workflow to transfer records from SPIRE has been documented and tested and there is confidence that the House administrations are approaching the point at which they will be able to carry out the first transfer from SPIRE. The process is designed to be driven by disposal triggers within SPIRE and is intended to be almost entirely automated, with metadata from the system used to create catalogue descriptions.

The existence of the Parliamentary Archives gives the House administrations the ability to adopt a unified approach for the management of the entire information lifecycle from creation to permanent preservation. In view of this, ensuring the survival and availability of records for the user of the future, via the digital preservation system, should be added as an objective to the Digital Strategy. See recommendation 1.