The National Archives

Information Management Assessment

Department for Work and Pensions

Reviewed

March 2015

Published

October 2015

Working with government
to raise standards in information management

Contents

Glossary

BSIRO – Business Senior Information Risk Owner

DPO – Data Protection Officer

DRO – Departmental Records Officer

DROID – Digital Record Object IDentification

DSOB – DWP Security Oversight Board

DWP – Department for Work and Pensions

EDSAC – External Data Sharing Advisory Centre

ERMS – Electronic Records Management System

ESA – Employment and Support Allowance

ERM – Electronic Records Management

FARIO – Find and Retrieve Information Online

FOI – Freedom of Information

HMRC - Her Majesty's Revenue and Customs

IAC – Information Asset Coordinator

IACSEP – Information Assurance and Cyber Security Engagement Programme

IAI – Information Asset Inventory

IAM – Information Asset Manager

IAO – Information Asset Owner

IM – Information management

IMA – Information Management Assessment

IMAB – Information Management Assurance Board

IMC – Information Management Consultant

JSA – Job Seekers Allowance

KIM – Knowledge and Information Management

KIMD – Knowledge and Information Management Division

KIRM – Knowledge, Information and Records Management

NINo – National Insurance Number

PIA – Privacy Impact Assessment

PIP – Personal Independence Payment

PST – Personal Storage Table

RM – Records management

SIRO – Senior Information Risk Owner

SLAQ – Series Level Appraisal Questionnaire

SPAG – Strategy Policy and Analysis Group

Stat-Xplore – tool for exploring benefits statistics

WSTB – Welfare Sector Transparency Board

Statement of commitment

The following statement was provided by the Permanent Secretary of the Department for Work and Pensions (DWP). It is published on the Department's intranet site.

Dear colleagues

Information is at the heart of everything DWP does, from processing claims for benefit, to helping people into work, assessing our performance against key targets, tackling fraud and error, developing policies and forecasting where we need to be in the future.

We also need to make sure that information on DWP customers are protected and used in a lawful and appropriate way, this often requires difficult judgement calls, most of the time we get these right but occasionally we do not.

To show the strength of the Department's commitment to getting these judgement calls right, I have asked The National Archives to review our information processes and systems. They have agreed to undertake this task in March 2015. The National Archives regularly conducts assessments of information management practices and compliance within government departments.

The report they produce will help me to support all aspects of information management across the Department so that our information is appropriately captured, managed and preserved and information risks and sensitivities are appropriately handled.

Yours sincerely

Robert Devereux
Permanent Under-Secretary, Department for Work and Pensions
22 January 2015

Information Management Assessment (IMA) background

The IMA involved a detailed review of supporting documentation followed by interviews with senior staff, specialists and practitioners in the Department's London, Leeds and Manchester offices and including a Job Centre and a Benefits Delivery Centre. These were conducted between 2 and 12 March.

The following report provides a summary of good practice and risks identified. IMA reports and departmental action plans are published on The National Archives' website at:

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

Key findings of the assessment

1 The value of information

Performance rating	
Communicating and realising value	**Development area**
Managing information as an asset	**Good**

- The Department for Work and Pensions (DWP) recognises the importance and value of its information and particularly the importance of protecting sensitive information. It has made excellent progress in the area of information exploitation. There has been positive support from senior management. For example, both the Permanent Secretary and Senior Information Risk Owner (SIRO) led a drive to promote the importance of records management (RM) and of complying with the print to paper policy.
- DWP has an information strategy (2012) in place which the Department has assured us is being updated, but does not have a central set of goals around corporate records management which fits within the wider strategic picture. This should be addressed in parallel to the current updating of the information strategy.
- Although staff recognise the importance of record keeping, they are still not consistently complying with the print to paper policy. DWP should seek to establish a senior champion for RM. This will help to raise awareness of the importance of RM and help promote the message that all staff have an important role in ensuring that the right records are kept and managed appropriately. **See Recommendation 1**.
- DWP has made excellent progress in establishing a process for information asset management and assurance. The Information Asset Owner (IAO) role was recently relaunched as the Business Senior Information Risk Owner (BSIRO) and there are well-defined responsibilities for the role. In addition, there are increasingly effective networks of Information Asset Coordinators (IAC) and Information Asset Managers (IAM). Information Asset Inventories (IAI) and

Information Asset Assurance Returns are regularly updated and reported on by IACs and IAMs. There have also been real attempts to incorporate information management (IM) and RM as part of this process; for example, the IAI includes information about retention and the Information Asset Assurance Returns include a question on compliance with the Records Management Policy. The majority of staff have completed the 'Responsible for Information' training and DWP are fully engaged with the Information Assurance and Cyber Security Engagement Programme (IACSEP).

2 Digital information and supporting technology

Performance rating	
Supporting information through technology	**Development area**
Digital continuity and IT change	**Development area**

- Although DWP manages its customer information well, the picture is less positive for its 'corporate' information. DWP does not yet have an Electronic Records Management System (ERMS), though there has been an aspiration to implement such a system for several years, and a print to paper policy is still in operation. Shared drives are widely used but there is no central Knowledge and Information Management (KIM) team oversight or control of these. Shared drives are not routinely well managed locally and they do not fully support the management of information throughout its lifecycle. Finding of information within business areas does not appear to be an issue, but sharing and finding information across these boundaries is often difficult. DWP needs to establish concrete plans to implement a central solution for managing corporate digital information. **See Recommendation 2**.
- In terms of digital continuity, DWP has a partial view of the corporate digital information it holds and requirements for RM have not always been part of projects to introduce new technology. The limitations of the current shared drive environment, inconsistent adoption of the print to paper policy; and a lack of oversight of control of corporate digital information, means there is a very real risk

that the organisation will not have the information it needs to carry out its business and may not be able to comply with information legislation and information assurance obligations. The organisation should devise a plan for embedding digital continuity (the ability to find, open, work with, understand and trust information for as long as you need to) into corporate business as usual processes. **See Recommendation 3**.

3 Information risk, governance and oversight

Performance rating	
Recognising information risk	**Development area**
Establishing control	**Satisfactory**
Providing guidance	**Good**
Measuring impact	**Development area**

- DWP has a solid process in place for managing risk, and information risk is recognised and managed, at least in terms of the security and protection of sensitive information. However, risks around the wider management of information and records are not yet fully recognised within the Department's risk management framework. DWP needs to ensure that it defines the risk of failing to manage its corporate information so that the impact of not capturing or keeping the information that is needed can be understood at all levels of the business and managed. The SIRO should have sight of this risk and the actions that are in place to manage it. **See Recommendation 4**.
- There is a good set of governance structures for information security through the DWP Security Oversight Board (DSOB) and the Information Management Assurance Board (IMAB). At present the structures are still maturing and in particular IM/RM related risk should have greater visibility in both the above Boards. However, with continued investment of effort from the centre of the Department plus support from the BSIROs they should provide an opportunity to bring senior people together and act as a forum for the recognition and

discussion of risks to information and mitigations.

- DWP has a comprehensive set of KIM policies and guidance covering the whole of the IM lifecycle, from creation, capture and what to keep, to management, disposal, Freedom of Information (FOI), data protection and information assurance. There have been good efforts to promote this across the organisation in an engaging and simple way through campaigns such as Essential Records Management and by producing shortened, easy to understand, 'desk aid' versions of the guidance. Many of the staff we spoke to were aware of the guidance and used it.
- There are relatively few formal measures in place at present to measure compliance with the Records Management Policy. A question on RM has been included in the Information Assurance Asset Returns and business areas are expected to provide evidence to demonstrate how they are meeting this. This approach is still maturing and the KIM team should define exactly what it wants business areas to report on. The Knowledge and Information Management (KIMD) Division also carry out file audits where over 400 registries are asked to provide lists of corporate registered files that they hold. If problems are found then these are escalated back up the management chain. These audits should be formalised as a method of managing compliance with the Records Management Policy. DWP should extend the audits to cover digital information; at the moment, due to key records being kept on shared drives rather than on registered files, they are only providing part of the picture. **See Recommendation 5**.

4 Records, review and transfer

Performance rating	
Oversight of records and selection	**Satisfactory**
Implementing disposal decisions	**Satisfactory**

- DWP has a robust and well established process in place for the oversight, control and management of its paper records. Considering that DWP transports, tracks and manages paper files on almost unrivalled scale across government, Capita (which manages the paper file stores in conjunction with the KIMD) meets user requirements and has a 99% success rate of being able to locate files. There is regular, controlled disposal of paper files. In order to comply with its obligations under the Public Records Act DWP also has very good processes for the appraisal, selection, sensitivity review, preparation and transfer of its paper records, is currently ahead in the transition to the 20-year rule and does not have a backlog.
- If we were assessing paper records alone we would consider DWP to be rated as good. However, improvements are needed in the management of its corporate digital information, hence the overall score of satisfactory. The KIM team does not have any control of the shared drives and has not yet started to consider how it might appraise, select, sensitivity review and transfer corporate digital information. Disposal is built into most of the benefits delivery systems but not all. It is therefore recommended that DWP works towards extending the KIMD oversight and control of paper records to digital information. The KIMD should do more to ensure that shared drives are being managed appropriately; in particular that information of value is being identified and kept for as long as it is needed, and that information is disposed of once it is no longer required.

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 management (IM) and records management (RM) related risks:

Highlights of the 2015 IMA
There is a good process in place for reporting on, and oversight of, information assets using the Information Asset Inventory (IAI) and the Information Asset Assurance Returns. The Information Asset Owner (IAO) role has been refreshed and relaunched as a Business Senior Information Risk Owner (BSIRO) and there was good practice around the Information Asset Coordinator (IAC) role and in establishing and maintaining good networks of Information Asset Managers (IAM). There have been real attempts to incorporate IM and RM into this process by including retention information on the IAI and a question on the Information Asset Assurance Returns around compliance with the Records Management Policy.
The Department for Work and Pensions (DWP) has a well-organised and successful system for handling Freedom of Information (FOI) and data protection and particularly effective networks of FOI Focal Points and Data Protection Officers.
DWP is increasingly proactive in sharing/making information available and there is a governance structure around this process. For example, it has established a substantial Data Warehouse which brings together the richest sources of customer and other public sector data and it exploits these as

much as it can. The analytical community brings in their own data and creates derived datasets from the warehouse. It is also used heavily for the process of 'data matching' which is helping to reduce fraud within the benefits/tax system.

DWP has also developed an online tool called Stat-Xplore, https://stat-xplore.dwp.gov.uk/, which provides a guided way to explore DWP benefit statistics. It currently holds data relating to Housing Benefit claimants, the number of National Insurance Number registrants entering the UK from overseas, Jobseekers Allowance and Employment and Support Allowance sanction decisions, and Personal Independence Payments. In future Stat-Xplore will include data on a wider set of DWP benefits.

DWP has a comprehensive set of Knowledge and Information Management (KIM) policies and guidance covering the whole of the IM lifecycle, from creation, capture and what to keep to management, disposal, FOI, data protection and information assurance. There have been good efforts to promote this across the organisation in an engaging and simple way through campaigns such as Essential Records Management and by producing shortened, easy to understand, 'desk aid' versions of the guidance.

Process management and oversight of paper records including records review and transfer is very good. DWP is currently ahead in its transition to the 20-year rule and has no backlog of review. They have an experienced and knowledgeable review team which plans ahead to meet transfer targets and is using more efficient methods of appraisal and selection, such as the Series Level Appraisal Questionnaire (SLAQ), in line with The National Archives' guidance. File audits are also providing the team with an effective way of tracking management of paper files within the business and tackling issues.

Recommendations to address risk areas

Recommendation 1
The Department for Work and Pensions (DWP) should ensure that it has a holistic strategy for corporate records management (RM) that reflects the value of information and importance of record keeping has greater profile and recognition across the organisation. This should be fully aligned with the wider Information Strategy.
This would be supported by: • Establishing a board level senior champion for RM. • Using the senior champion for RM to promote the strategy across the organisation. • Developing a RM strategy that includes a message to staff at all levels about their responsibility for RM. • Aligning the RM strategy with the wider information strategy and with Information Assurance and IT. • Ensuring that work to develop a new Electronic Records Management (ERM) solution is a core part of this. • Defining critical success factors for the new strategy. • Developing an implementation plan for the strategy.

Recommendation 2
DWP needs to establish concrete plans to implement a solution for managing unstructured corporate digital information to replace the print to paper policy.
This would be supported by: • Defining business requirements for RM, for example, around search, data sharing, metadata, access management and disposal, and that they guide the implementation of an Electronic Records Management System (ERMS). • Collaborating and learning from the experience of other departments that have recently rolled out ERM solutions. A plan to identify key corporate information on the shared drives and migrate this to the new ERMS, to freeze shared drives to

new content once the ERMS has been rolled out, and switch off the shared drives once the new system is established.

- Training and supporting staff in using the new ERMS.
- Ensuring that the new ERMS connects to the email system and make the process of saving significant emails as easy as possible for staff, automating the process where possible.
- Applying retention rules to Enterprise Vault. For example, one government department disposes of information in Vault after two years. Making sure staff are aware of this, and are reminded of the need to save emails of corporate value to shared drives and/or print off and put on registered files.
- Applying retention rules to Lync and making it clear to staff for what exact purpose they should be using this system.
- Ensuring that there is a process for capturing any key corporate information from Drupal, applying retention rules, and making it clear to staff exactly what they should be using this system for.

Recommendation 3

DWP should devise a plan for embedding digital continuity (the ability to find, open, work with, understand and trust information for as long as you need to) into business as usual processes.

This would be supported by:

- Fully recognising and managing risks to the continuity of digital information as part of the risk management process.
- Building digital continuity into the information asset management process as suggested in the 2011 DWP Digital Continuity Policy.
- Surveying digital information held on shared drives as part of the preparation for moving to an ERMS. This could be done in a similar way to the paper file audits, asking business areas to report on what is held in the shared drives.
- Negotiating a slot to run The National Archives' Digital Record Object IDentification (DROID) tool, or similar, would be particularly helpful in determining how much duplicate information is held and in identifying formats and age of information.
- Ensuring that Knowledge and Information Management Department (KIMD) staff are involved in any IT developments that would have an impact on KIMD responsibilities from the outset and that business requirements for IM are a core part of these projects. Business requirements would include, for example, whether you can add the correct metadata, whether there is adequate search functionality, whether you can export or dispose of information and manage access restrictions
- Ensuring that the need to keep information within benefits delivery systems

available and usable is factored into DWP's plan for implementing digital continuity as business as usual.

Recommendation 4

DWP should factor IM and RM into the way it defines and monitors information risk.

This would be supported by:

- Ensuring that that the risk of not capturing and keeping the records it needs, in the way that it needs for as long as it needs, is recognised and managed through the risk management framework.
- Ensuring that information risks are discussed at the Information Management Assurance Board (IMAB) and are given scrutiny by the DWP Security Oversight Board (DSOB).
- Promoting awareness of information risks and how they should be managed.

Recommendation 5

DWP should seek to establish a more effective approach to monitoring and achieving compliance with IM and Records Management Policy.

This would be supported by:

- Establishing a network of information representatives or KIRM advocates across the organisation. This should include a role description and training and support from the Knowledge and Information Management (KIM) team.
- Using this network to promote KIM policy and processes and provide training and support for staff on information and records management in business areas.
- Building on the work that has already been done to monitor compliance with the Records Management Policy using the Information Asset Assurance Returns in particular, further defining what sort of evidence business areas should provide in order to demonstrate compliance.
- Gaining greater assurance on the content of shared drives and the management of this content by, for example, by extending file audits or building into the Information Asset Assurance Returns.
- Considering rolling out the Essential Records Management campaign of bite-sized information on IM and RM across other business areas.

Recommendation 6
DWP should work towards extending the KIMD's oversight and control of paper records to digital information.
This would be supported by: • Exploring the possibility of extending the paper file audits to cover digital information on the shared drives, and as part of this, ask business areas to report on disposal. • Ensuring that all digital systems (including benefits delivery systems and the new ERMS) have disposal built in and that disposal is being actioned. • Ensuring that the KIMD/information advocates in the business are involved in the creation and management of shared drives. • Beginning to devise an approach for appraisal, sensitivity review and transfer of digital information, particularly that on the shared drives, drawing on advice from The National Archives and other government departments' work in this area.

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 Department for Work and Pensions (DWP) recognises the importance and value of its information and particularly the importance of protecting sensitive information. The Records Management Policy clearly states that all staff are responsible for record keeping and clearly sets out which records should be kept, why and for how long. This is mirrored throughout related policies, guidance and training. DWP is undertaking a substantial Business Transformation Project and information is an integral part of this and the vision for how DWP will be operating by 2020 through the Intelligent Data Use Sharing and Management strand.

The outgoing Senior Information Risk Owner (SIRO) has been engaged with information management (IM) and in June 2014 submitted a paper on the importance of record keeping, what should be kept and adhering to the print to paper policy, to the Executive Team. The Permanent Secretary then wrote to all staff to remind them of their records management responsibilities. The SIRO chairs the DWP Security Oversight Board (DSOB), which provides assurance and governance for all security issues across the Department.

Almost all of the staff we spoke to recognised the importance of the information that they create as part of their work. There was a particularly strong recognition of this among those working with customer records at the delivery end of the business. However, despite the write round from the Permanent Secretary and continual reminders from the Knowledge and Information Management Department (KIMD), staff are still not consistently complying with the print to paper policy and are using the shared drives and email instead. Several interviewees felt that the promise of a

digital solution for records management (RM) being 'just around the corner' for many years had 'put people off' from printing to paper. Others felt that it just did not fit with the way they work. Printing off digital records was just an additional task that they did not have the time to perform.

There was also a feeling that the loss of the Administrative Assistant grades, which used to be responsible for registered filing, had contributed to the breakdown of the paper system. Several interviewees felt that more could be done, particularly at senior levels, to push the message that 'we are all information managers.' One interviewee wanted to see 'a global emphasis on filing as part of your responsibilities as a civil servant, like you do in information security.' Another felt that 'the whole Department has to be engaged in IM and RM…there has to be a bottom up as well as a top-down approach.' This message should form an important part of any new RM strategy. In addition DWP would benefit from having an established senior champion for RM. This role should ideally be at board level and could be the SIRO, but does not have to be. This would help to ensure that the importance of IM and the risk to the business if it is not done well is recognised at the highest level, and that there is someone senior enough to promote this message across the organisation. **See Recommendation 1**.

Setting goals for information and its management

DWP is providing direction for many aspects of managing its information. The DWP has an Information Strategy which was implemented in 2012, and is based around the seven Cabinet Office information principles. Work on a refreshed information strategy has now been tied to the emerging priorities of the Business Transformation Group. The aim is to update the strategy and to ensure that it is aligned with the 2020 digital vision. However DWP does not have an underpinning corporate records management strategy. DWP should develop such a strategy that includes a message to staff at all levels about their responsibility for RM. The strategy should set clear critical success factors and have a clear plan for implementation This should be aligned with the work to establish an Electronic Records Management (ERM) solution for corporate records. **See Recommendation 1**.

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

DWP has a well-organised and robust system in place for handling Freedom of Information (FOI) requests, which is borne out by FOI figures. DWP reported having received over 1,000 requests in Q3 2014 – in fact, it has received over 1,000 requests every quarter since Q3 2012. Of those received in Q3 2014, 90% met the 20-day deadline and 90% were answered in 'time' (meeting deadline or within permitted extension). From Q1 2013, DWP has consistently achieved a figure of 90% answered in 'time' for every quarter. In Q3 2014, 65% of resolvable requests were granted in full – this is above the average for all monitored bodies (49%). 28% were withheld in full, which is slightly below the average for both departments of state (33%) and all monitored bodies (32%).

Both FOI and data protection activities are coordinated centrally but the process of handling individual requests is devolved to networks of FOI Focal Points and Data Protection Officers (DPOs) and Deputy DPOs. Staff we spoke to felt that this process works well because the business has greater knowledge of its information and likely sensitivity issues. Requests are logged and tracked using a workflow system, records of the process are kept and retention is built in. The central FOI and Data Protection teams provide advice, guidance and support to FOI Focal Points, DPOs and Deputies via the intranet and through regular telekits or video conferencing sessions. The central teams are also looking at innovative ways of extending their reach, for example, FOI Focal Points have a virtual team and the Data Protection team are helping DPOs to help each other by setting up mentoring sessions. It is recommended that the Knowledge and Information Management (KIM) team investigate the possibility of using some of these methods when establishing an effective network of Knowledge and Information Management Department (KIMD) advocates. **This is good practice**.

Despite the sensitivity of much of its information, DWP is striving to proactively publish as much data as possible and has made real progress in this area. **This is good practice**. As at 23 February 2015, there were 4,086 publications by DWP on

GOV.UK, 203 of which were classed as transparency data. The Department has published 292 datasets on data.gov.uk. The website gives the Department an average score for openness of 0.2 and has received a total of 49 stars.

There is recognition of the potential tensions between transparency and security and these two areas are together under one Director General Command. DWP has established a Welfare Sector Transparency Board (WSTB). This is external facing and includes financial people from work programme contracts and representatives from blue chip companies. All records of this group are published. There is also an Open Data Working Group which sits underneath the WTSB and includes representatives from their main consumer groups. This group helps DWP to understand what consumers of their information want and understand their priorities as well as acting as a forum to discuss what they can do better as an organisation and where changes can be made.

There is a good governance structure in place around the sharing of information. All external data sharing requests from other Government Departments come through the External Data Sharing Advisory Centre. There is also a Data Ethics Committee consisting of internal and external members and chaired by Head of KIMD.

The Department has established a substantial Data Warehouse which is a rich source of customer data, lawfully obtained from its own and other public sector sources. DWP exploits this in order to fulfil its functions and additionally to forecast, evaluate, develop polices and processes, produce fiscal frameworks and predict trends and future needs in accordance with its own legislation.

The information is derived from DWP, Her Majesty's Revenue and Customs (HMRC), Northern Ireland Social Security Agency and Local Authorities but is enriched with other public sector data where this can be reused. It is therefore a highly sought after resource across government statisticians and analysts and the wider analytical community.

Access to this is controlled and wherever possible anonymised for further use. Where personal data needs to be used it is done so in accordance with strict procedures, processes and controls. The environment enables analysts to develop

further datasets from and within the warehouse where further use is likewise controlled.

It is used by other government departments such as HMRC and also used heavily for the process of 'data matching' which is helping to reduce fraud within the benefits/tax system.

DWP has also developed an online tool called Stat Xplore https://stat-xplore.dwp.gov.uk/ which provides a guided way to explore DWP benefit statistics. It currently holds data relating to Housing Benefit claimants, the number of National Insurance Number registrants entering the UK from overseas, Jobseekers Allowance and Employment and Support Allowance sanction decisions, and Personal Independence Payment. In future Stat-Xplore will include data on a wider set of DWP benefits.

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

DWP has made excellent progress in establishing a process for information asset management and assurance. According to the Information Asset Manager (IAM) Guide, which is available on the intranet:

> *An information asset is any piece or collection of information, stored within the DWP estate, defined and managed as a single unit so that we can understand it, share and protect it effectively and get the most value from it. It is something we cannot replace without cost, time, skill and resources.*
>
> *It may be customer data or employee information but it is not only about personal information. It includes any type of information that, if lost or*

misused, could affect our ability to deliver services, or could damage the Department's reputation e.g. commercial documentation.

This is a good description that reflects the government definition of an information asset and ties in with the DWP Records Management Policy and related guidance and training. The fact that it explicitly states that it is not just about personal information is very helpful, as we have seen information asset approaches that are based largely around only this type of information. The description provides a good basis for building IM and RM into the asset management process and encourages business areas to think about information in its widest sense.

Each Business Senior Information Risk Owner (BSIRO) has their own Information Asset Inventory (IAI), which is the DWP equivalent of an information asset register. IAMs are responsible for reviewing and keeping IAIs up to date and the Information Asset Coordinators (IAC) oversee this process.

DWP uses IAIs to identify and track its information assets. There is a standard IAI template available on the intranet. This is quite detailed and includes details about the system/asset, owners and contact details, data transfer where relevant, what type of information the system/asset contains, accreditation, the impacts on confidentiality, integrity and availability and retention information. IACs are responsible for checking that IAIs are populated and kept up to date. Staff we spoke to reported that the quality of information in these varies (the example we saw was detailed), some are very good, some less so, and one IAC said that they often had to chase IAMs to get retention information added. The IAI is recognised as an important tool for DWP and one interviewee working in the area of information exploitation said 'the Department needs to know what we hold so we can properly exploit it.' **This is good practice**.

Ownership of information assets

The BSIRO role was established in 2014 and built on the existing role of IAO. This is a senior role, usually at Director level, though it has also been applied to particularly important projects. There is a role description/performance objective for BSIROs which states that they are responsible for:

- *Demonstrating professional and visible leadership, ensuring senior management focus on all information management, assurance and security-related issues;*
- *Leading and fostering a culture that values, uses and protects information for the public good, through proactive communication;*
- *Taking the lead for the effective management and mitigation of information risks, including the maintenance of a business-specific information risk register and ensuring individual business risk decisions are consistent with the DWP information risk appetite;*
- *Overseeing the management, reporting and escalation of information or security incidents, ensuring that breaches are dealt with fairly and consistently; and*
- *Providing an appropriate level of assurance to the DWP SIRO through endorsement of the through-year information security and assurance reports.*

The BSIRO guide states that they need to know:

- *What information is held in their part of the business*
- *In what format information is held, transferred and destroyed*
- *What information is added or removed*
- *Who has access to information assets and why*
- *Who is responsible for managing those processes within the business*
- *What are the risks to the information*

BSIROS are expected to attend and participate in the Information Management Assurance Board (IMAB) meetings. Staff we spoke to said that these meetings provided an opportunity for BISIROs to provide updates and to share best practice, lessons and discuss points of accountability. One BSIRO who was relatively new to

the role reported that they had ‘buddied’ up with BSIRO from another Directorate to learn more about the role in practice.

Given their seniority, it is recognised that BSIROs will not be able to be involved in the day to day running of this process. They are therefore supported by IACs and they, in turn, are supported by networks of IAMs across the business. IAMs are responsible for compiling and maintaining the IAIs and update them twice a year. IAMs are also responsible for gathering and sending evidence for the twice-yearly Information Asset Assurance Returns to their IAC. The IACs coordinate this process and are responsible for passing Information Asset Assurance Returns to the BSIRO. The IACs we spoke to were committed to the role and proactive both in terms of fulfilling their information assurance reporting requirements but also in coordinating networks of IAMs in their business areas and providing training, updates and support. One IAC described how they provide links to training and guidance and provide training sessions for the IAMs and are considering the possibility of rolling this out to IAMs across DWP. As is often the case these responsibilities are something that IACs and IAMs do on top of already busy day jobs. The level of the IAM role varies throughout DWP, according to one IAC, it should be at Senior Executive Officer level and there is some concern among IAMs about balancing their work with the demands of the role and awareness of importance of this work.

The Information Asset Assurance Returns are comprehensive and include questions on five of the six areas that are reported on annually across DWP: leadership and governance, training education and awareness, information risk management, through life information assurance measures and assured information sharing. In terms of a sixth area, compliance, an appropriate checking regime is being developed to demonstrate compliance with departmental policies and procedures. The returns are more than just a box ticking exercise, as business areas are expected to include evidence to demonstrate how they have met their obligations. The example we saw has a detailed response and evidence for each question. DWP has also attempted to build IM and RM into the Information Asset Assurance Returns by adding a question about whether the DWP Records Management Policy is applied appropriately. This is a positive start but as it is quite high level it is recommended that some KIM staff work with Information Assurance to further define

exactly what is meant by this question and what evidence is required, to enable IACs and IAMs to provide a more useful response.

DWP is fully engaged with the Information Assurance and Cyber Security Engagement Programme (IACSEP) run by The National Archives. The IACSEP team reported that they have trained a number of the BSIROS and have also hosted an away day for IAMs. The DWP Head of Security and Business Continuity attends all their events and contributes to the e-newsletter.

2 Information and supporting technology

2.1 The technology environment

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

Corporate storage of information

The Department for Work and Pensions (DWP) does not yet have an Electronic Records Management System (ERMS) and a print to paper policy is still in operation, though there has been an aspiration to implement such a system for several years. Plans to bring in a collaboration tool and in the longer term use as an Electronic Records Management (ERM) solution, were halted at the end of 2014. DWP is now aiming to build a system both for collaboration and information management (IM) and records management (RM). According to one interviewee consideration has been given to go open source as it will 'give DWP the flexibility to work in the way that they need to.' This work should form a core part of a new RM strategy. DWP should ensure that it has clearly defined its business requirements for IM (for example, around access, disposal, and search), and that these guide the implementation of the new ERMS. In addition, it should also make contact with and learn from the experience of other departments which have recently rolled out new ERM solutions. A lot of time and effort was spent preparing to bring in the collaboration tool including, for example, creating a new file plan. As this work was function-oriented it can be reused for whatever new system is chosen. **See Recommendation 2**.

Shared drives

In the absence of an ERMS, shared drives are used to store and manage unstructured information. These have been in existence for around 20 years and staff increasingly use them to store key corporate information rather than printing it

off and putting it on registered files. There is some brief central guidance but decisions about how shared drives are structured and managed are made at the local level. The Knowledge and Information Management Department (KIMD) has no oversight or control of the shared drives and their influence here is limited. For example, IT handles requests to set up new shared drives without recourse to KIMD.

Access to individual shared drives is limited to the relevant business areas so the information within them is not accessible across DWP. According to one interviewee the only real way of sharing information is by email so there are 'multiple versions all over the place with no control over and no responsibility for the finished article and what is done with it.' Another stated that everyone has their own way of doing things, that personal file naming was frequently used and that there were files that needed to be disposed of but no time to do it. There were also concerns around a lack of 'future proofing' - for example, if teams are reorganised it would be difficult for successors to understand what information is in the shared drives and how it is organised.

Disposal from shared drives has to be performed manually by individual business areas and practice is patchy. There is also an issue with 'orphaned' shared drives when teams disband and there has been pressure from IT to delete these shared drives. KIMD has had to insist to IT that they review the drives before deletion as they may contain key corporate records.

There was a general recognition amongst KIMD and IT that the shared drives would need to be frozen and eventually switched off to ensure take up of the new system. In addition to this, DWP should ensure that there is a plan to identify and migrate key corporate information from the shared drives to the new ERMS and to dispose of what is no longer required. This work needs to be a concrete part of plans to establish an ERM solution as part of a new information strategy. **See Recommendation 2**.

Benefits delivery systems

The majority of DWP's digital information is held within line of business systems designed to manage the process of benefits delivery. The records that reflect the benefits delivery process are increasingly digital – either because they are received/created digitally or scanned into the Document Repository System. Some of these rely on old technology and many of them interconnect (see Section 2.2). Most of these systems have disposal processes built in, but there are some exceptions to this. (see Section 4).

Emails

According to the Email Management Desk Aid, emails must be 'maintained as records in accordance with the Records Management Policy.' There are limits on email inbox size of 200mb but some staff we spoke to said their limit had been increased. Use of Personal Storage Table (PST) files to store emails was widespread despite a warning that these are not supported and there is a real risk that key corporate information will be lost. One interviewee said 'I know I shouldn't use PST files, but I do.' Enterprise Vault will soon be implemented to try and discourage the use of PSTs by providing backup storage of email. According to policy, 'significant' emails and attachments should be printed out and put on registered files. Some staff said that they saved significant emails to their shared drive but very few said that they printed emails out to put on registered files. There is a risk therefore that key corporate records are not readily accessible to staff or being kept for the requisite period of time and that emails of potential historical value will not survive to be selected and transferred to The National Archives. The Department has also recently rolled out Lync for instant messaging, although they have yet to make decisions about how long to keep the messages within this and to issue guidance on what Lync should be used for. DWP should ensure that the new ERMS connects to the email system and make the process of saving significant emails as easy as possible for staff, automating the process where possible. Retention rules should be applied to Enterprise Vault (for example, one government department disposes of information in Vault after two years) and staff should be reminded of the need to save emails of corporate value to shared drives and/or print off and put on

registered files. Retention should also be applied to Lync and staff need to be clear on exactly what they should be using this for. **See Recommendation 2**.

Collaboration systems

DWP has been using Yammer as a collaboration tool for around two years. This has been replaced by Drupal. There is a user guide for Yammer which states that information within the system is considered to be part of the DWP record, however this is for Freedom of Information (FOI) purposes. In practice staff can delete posts as they see fit. The Records Management Policy states that only ephemeral discussions can take place on Drupal therefore it is not anticipated that significant posts will be on there. However, it is intended to make the point clearer in the next review of the policy. In implementing Drupal, DWP should ensure that there is a process for capturing any key corporate information for the record and that retention rules are applied. They should also ensure that staff are clear on exactly what they should be using the system for. **See Recommendation 2**.

Finding, accessing and protecting information

Although many staff we spoke to managed to find and share the information they needed within their own business area, there are barriers to information sharing across teams, as information held within shared drives, email inboxes and PST files is not accessible across the organisation. Information sharing across teams is largely done by email. The implementation of an ERMS, a well-structured and easy to use file plan; and the eventual closure of the shared drives has the potential to improve the situation as long as it is done well. Capturing the right metadata will also help to improve the findability of information both in the new ERM solution and in terms of how staff are naming information on the current shared drives. DWP should also ensure that the new system has sufficient search functionality and that staff know how to get the best out of this. **See Recommendation 2**.

The shared drives present some issues around access permissions where staff have moved business areas but can still access the shared drive of their former team. It is

the responsibility of business areas to keep track of who can and cannot access their shared areas. In contrast there seem to be good controls around access and privileges for benefits delivery systems which contain large amounts of sensitive personal data. Interviewees were generally confident that systems were set up to keep information secure. For example, according to one interviewee 'Customer Management System (CMS) is not a general access system. Only certain people have access and what they can see depends on their privileges.' In rolling out its new ERMS, DWP should ensure that access controls can be applied and maintained. **See Recommendation 2**.

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

DWP has a Digital Continuity policy produced in 2011. This is very comprehensive and covers areas such as risk assessment and mitigation and the use of Information Asset Inventories (IAI) to record and manage this, applying retention policies and complying with security standards. The policy was aimed at operational and transactional systems, analytical digital datasets, end user computing (EUC) applications and web content. It excluded digital information that should be printed to paper and put on registered files. It was unclear exactly how far this policy had been implemented across the business. The sample IAI we were provided with does include a risk rating for confidentiality, integrity and availability but this is from an information assurance perspective rather than digital continuity. Digital continuity risks are not yet fully defined within the DWP risk management process (see Section 3). One interviewee said that there is an aspiration now to move away from a standalone policy and ensure that digital continuity is built into business as usual but it was not clear how this would happen. It is therefore recommended that DWP devise a plan for implementation. The plan should cover all digital information,

including that on shared drives, as DWP cannot guarantee otherwise that significant corporate information has been printed and put on registered files. **See Recommendation 3**.

There has been work in conjunction with DWP's IT supplier to map the technology environment, which has enabled a better understanding of the applications in use across the organisation and their functions. DWP only has a partial view of the digital information it holds, which is largely due to the lack of oversight of information within shared drives. It is recommended that DWP survey the digital information held on shared drives. This could be done in a similar way to the paper file audits (see section 4), asking business areas to report on what is held in within the shared drives. Negotiating a slot to run Digital Record Object IDentification (DROID) software (or a similar tool) over the shared drives would also be helpful particularly in terms of determining how much duplicate information is held and identifying formats and age of information. Understanding what information you hold and identifying what needs to be migrated is an important part of moving to an ERM solution and should form part of DWP's work to move to a new ERMS. **See Recommendation 3**.

Digital continuity planning/IT change

In the past, IM and RM requirements have not always been given the right emphasis in IT projects. Going forward, DWP should ensure that KIM considerations are routinely part of plans to bring in new systems from the outset and that business requirements for IM (for example, can you add the correct metadata, is there adequate search functionality, can you export or dispose of information, can you manage access restrictions) are a core part of these projects. **See Recommendation 3**.

There is good practice around ensuring that information in benefits delivery systems remains available and usable. One interviewee described their work around the Customer Information System (CIS), which provides a single and accurate view of key data held for all DWP customers, is at the heart of the Department (101 million customer records). The CIS provides a picture of a customers business with DWP,

enabling the collection of personal customer information only once and sharing with DWP systems as well as other government departments. It is the master system for this information, connects with 40 other systems and there has never been a fundamental failure. DWP believes this is down to 'good design based on requirements, comprehensive assurance and testing and a good relationship with supplier.' CIS is ten years old but the Department is remediating the hardware and moving it to the most up to date version of Oracle by next year. Due to the number of benefits delivery systems used across DWP, it was not possible to establish whether all systems were being managed and maintained in this way and certainly several interviewees raised concerns about the age of the systems. However, there did seem to be a general recognition of the importance of keeping this information available as it was crucial in carrying out DWP's core business functions. Also, some of the systems are simply being maintained in the short term, as they will ultimately be superseded by Universal Credit. DWP should ensure the need to keep information within benefits delivery systems available and usable to be factored into DWPs overall plan for implementing digital continuity as business as usual. **See Recommendation 3**.

3 Information risk, governance and oversight

3.1 Recognising information risks

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

Documenting and defining information risks

The Department for Work and Pensions (DWP) has nine risk categories: strategy risk, governance risk, financial risk, legal and crime risk, change risk, customer service and operational risk, information risk, people risk and communication risk. Information risk is described as:

> *Risks arising from inadequate management of information used to support service delivery, decision taking in line with accountabilities and to ensure delivery of DWP and government objectives.*

There are six categories of risk associated with this: confidentiality, integrity, availability, economy, effectiveness and efficiency.

In practice, information risk tends to be defined as risks to the security of information, particularly sensitive personal information. The risks detailed on the Information Management Assurance Board (IMAB) risk register reflect risks around the protection, security and sharing of information, and around the physical loss or corruption of paper information. In relation to this, it recognises a range of potentially significant consequences including reputational damage, legal actions, sanctions or financial penalties. However, there is nothing on the risk of not capturing and keeping the records it needs, in the way that it needs for as long as it needs. For example, the risk that significant corporate information is not being captured onto registered files but being kept on shared drives is not reflected here, nor are risks around not being able to access or use information help within legacy systems.

The impact of a records management (RM) failure may have a significant effect at a team or even at an organisational level if information is not available in the way that it should be. The records review by Sir Alex Allan (2014) emphasised the importance of organisations to be able meet obligations for the appraisal and review of records. In the short to medium term there can also be significant impact in business terms if a Department cannot justify or explain decisions that have been taken or does not dispose of information when it needs to. However, DWP is not currently subjecting information management or RM- related risks to scrutiny or monitoring processes to manage them through the risk management framework. As a first step, DWP needs to ensure that it defines the risk to the Department of failing to manage information so that the impact of not capturing or keeping the information that is needed can be understood and managed at all levels of the business. The Senior Information Risk Owner (SIRO) should have sight of this risk (via DWP Departmental Security Oversight Board (DSOB) and IMAB) and the actions that are in place to manage it. **See Recommendation 4**.

Implementing an information risk management approach

DWP processes personal data on a very large scale. It follows a four-stage approach to managing risk:

- Identify risks, causes and consequences and document them on the risk register.
- Assess the potential impact and likelihood of each risk, prioritise (on a risk register) with inherent and residual risk scores, and a documented understanding of existing controls to mitigate risk and the effectiveness of those controls.
- Agree a strategy/approach for addressing key risks, identify owners and document on the risk register.
- Regular risk reporting to management, for example, reports to executive management, summarising the key risks and risk portfolio of the Department as a whole.

Most risks are managed at strand/project level. However, escalation is encouraged when the risk cannot be managed effectively at that level, or where control is outside the area / direct influence of the Risk Owner and a decision is required at a more senior level. The Escalating Risk guidance also states that risks can also be escalated for communication only, to advise senior management that a risk with a potentially significant impact exists and, where possible, provide advice on how it is being managed. In all circumstances it is for the senior manager to ensure that sufficient mitigation is put into place or, where the risk is significant, to consider whether the information should be used. In some circumstances it may be appropriate to highlight separately to the Business Senior Information Risk Owner (BSIRO) or SIRO that a risk is considered to be so high that it is, for example, unlawful. It is important that significant risks have adequate visibility at a senior level. All projects have to complete a Privacy Impact Assessment (PIA) that is designed to flush out key risks to information. This has three effects: compliance with Cabinet Office directive for information use and accountability, good practice as identified by the Information Commissioner, and provides a public facing document should there be a request under the Freedom of Information Act.

The IMAB offers a useful forum for senior business representatives to surface and discuss information risks in their capacity as BSIROs. The BSIROs we interviewed suggested that although information risks were meant to be covered at IMAB, in practice there was little discussion of this. Above this, the DSOB 'heat map' is designed to map all security and information risks at a high-level. However, on the version we were given IM or RM risk does not appear to feature either as a standalone risk or as a contributory factor in individual security risks. We understand that information security is on the agenda for every Audit Committee meeting, with one interviewee noting that the committee recognised it was an area that it needed to understand and had to be on top of. However, here again information and records management related risks are not yet receiving scrutiny. DWP has an excellent range of controls in place for information security, and a good set of structures for monitoring through the DSOB and the heat map, but it should build IM and RM risk into this process. In overall terms, DWP needs to be confident that strategy is in

place that prioritises IT systems as a means of supporting information, and that risks have been identified. **See Recommendation 4**.

3.2 Establishing control

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

Governance structures

DWP has a good governance structure in place for information assurance and IM. DSOB provides assurance and governance for security issues across DWP. It sets the direction for security strategy, concentrating on the big issues and key risks for the Department, and is the strategic decision-making body and escalation route for significant security issues. The Board's remit encompasses all aspects of departmental security: strategy, governance, technology, operational, information, people, process and risks. DSOB is chaired by the SIRO and its membership consists of, Digital Transformation Director General, IT Director, Operations Director, Universal Credit Programme Director, Chief Security Officer and other attendees such as the Chief Technology Officer, Departmental Security Officer and Chief Internal Auditor.

IMAB reports into DSOB and its purpose is to:

- oversee policy, guidance, support and assurance relating to information management and security; and

- ensure that DWP and its arm's-length bodies are adhering to legislation, other mandatory requirements and central guidance; and pursuing best practice in appropriately balancing their need to protect and exploit information while delivering Departmental objectives.

IMAB is currently chaired by the Director of Data and Analytics and its membership is largely made up of BSIROs. **This is good practice.** At present the governance structures are still maturing and in particular information risk should have greater

visibility in both boards. IMAB and DSOB with continued investment of effort from the centre of the Department plus support from the BSIROs, they should provide an excellent opportunity to get senior people together and act as an important forum for the recognition and discussion of risks to information and mitigations.

At the time of this assessment, the SIRO role was in the process of moving to the Director General for Technology. The incoming SIRO recognises the importance of IM and requested that the Directorate which hosts the Knowledge and Information Management (KIM) function be moved to Technology. This has now been implemented. Staff we spoke to as part of the assessment felt this to be a positive move and, in particular, thought it would help to ensure that KIM considerations are recognised and incorporated in IT projects from the start.

Supporting the business

The Knowledge and Information Management Department (KIMD) sits within the Data and Analytics Directorate. This and the Security Directorates have moved from the Finance Group to Technology which should improve links with IT (seen as a positive move by staff). The KIM division consists of the following areas: Freedom of Information (FOI) and Open Data, Data Sharing and Data Protection Policy, Records Management, Information Strategy and Data Governance, External Data Share Advice Centre and DWP Library Services. The Departmental Records Officer (DRO) leads the KIRM team. Focus for the team in the past year has been around preparing for a collaboration tool (to include Electronic Records Management (ERM) functionality) , improving compliance with the print to paper policy, paper reduction and retention policy.

Due to the size of the organisation, KIMD support to the business is provided largely through guidance and training given on request. Areas such as FOI and Data Protection rely on networks to carry out their work (see Section 1) and KIMD too would benefit from an effective network of information representatives. This would improve the reach and impact of the KIMD in the business (see ‘Support networks’ on page 40).

Support networks

DWP does not yet have an effective network of Records Management (RM) representatives out in the business. There are Nominated Contacts but in practice these are used largely as a point of contact for the paper file audits. There is an aspiration to establish a network of KIMD advocates across the organisation and it is strongly recommended that DWP works to make this a reality. This could be by establishing a new network or building on one that already exists, for example, this could be built into the role of the IAMs. Networks of this kind, particularly in very large and geographically distributed departments like DWP, are essential to extend the reach of the KIMD and help to promote, implement and monitor KIM policy and practice. They also play a crucial role in the implementation of ERM systems, helping to promote the system and train and support staff in their business areas. There is some good practice around networks developed for FOI and Data Protection and information assurance (see Section 1) that DWP can draw on. Also, a KIM Champions network has been established within Strategy Policy and Analysis Group (SPAG). These Champions develop an action plan assessing how good KIM practice is in their area and how to improve it. There are also monthly meetings to discuss issues and share best practice. **See Recommendation 5**.

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

DWP has an up-to-date Records Management Policy which is available on the intranet. This covers principles around keeping corporate and benefits records including the print to paper policy, assurance and compliance, where documents should be stored for and how long and KIM contacts. It also clearly states that:

All staff have a responsibility to keep records of the decisions they make, the advice they give, anything they do in the course of their work if it is significant.

The policy makes it clear that the print to paper approach is still in operation and must be followed:

All 'significant' corporate records must be printed to paper. Any electronic document, including emails and Intranet documents, must be printed to paper and put in a Registered File or Corporate Record Box as soon as it has been identified as a 'significant' record.

There is a wealth of other KIM policies and guidance covering all aspects of the RM lifecycle. These are all available on the intranet and many of the staff we spoke to knew about them and used them. Much of the guidance has also been broken down into 'desk aids' to make it easier to understand and help staff have the guidance to hand as they carry out their work. **This is good practice**.

There have been concerted efforts by the KIMD to raise awareness of the Records Management Policy and promote the guidance. Records Management Extra gives a fascinating overview of the life of a registered file from what records staff should be keeping, through the stores at Heywood, then the selection, preparation and transfer process and finally preservation at The National Archives. The Essential Records Management campaign consisted of bite-sized chunks of content issued over five weeks for staff within Finance Group on subjects such as the importance of RM and dispelling myths about record keeping, the print to paper policy, disposal and life of registered file, Find and Retrieve Information Online (FARIO) system, roles and responsibilities for KIM, The National Archives, FOI and Parliamentary Questions. **This is good practice**. There is an aspiration to roll this out across other business areas within DWP and the organisation should definitely pursue this. **See Recommendation 5**.

What to Keep

DWP has produced some good general guidance on what to keep and about the type of documents that should be kept for the record. The 'What to Keep Guide' gives high-level guidance on the types of records that should be kept and advice on what should be put on a registered file. There is also a desk guide on 'What we should have kept May 2010-2014' which provides a list of the work areas/activities that should be stored in Registered Files as a departmental record. These principles are mirrored throughout the KIM policies and guidance described earlier. They have also developed an organisation-wide disposal schedule covering key types of records found across DWP. What to Keep is also covered by KIM training and in guidance campaigns such as Essential Records Management and Records Management Extra.

In a separate but related piece of work, the Pace team in the Operational Excellence Division had worked with the KIM team to map the business process for paper customer records. They examined the whole process and the record outputs in order to create a 'blueprint' for the customer journey. They are now creating guidance and desk aides and looking at how they can monitor whether staff are following this. **This is good practice**.

There was a good recognition among staff we spoke to of the need to keep records of their work. We found evidence that staff were using the guidance and one member of staff when asked whether there was any guidance to help them decide what information had value, referenced the desk guidance that he had been pointed to by a member of his team and said that he had it on his desk. In particular there seemed to be very clear knowledge about what customer records needed to be kept at the delivery end, where and how long for. In terms of its corporate information (non-customer information) the key issue for DWP is not 'what' to keep but 'where' to keep. Many staff we spoke to were keeping records on the shared drives rather printing them to paper and putting them on registered files as instructed. Several members of staff reported a particular issue around the management of project records. One member of staff on taking over responsibility for a particular project said it took him six months to piece together the records of that project from various

sources such as shared drives, email, personal drives, and registered files. Some staff we spoke to suggested that there was probably a tendency to keep too much; for example, one interviewee felt that the problem was 'not a lack of documentation but seeing the wood for the trees', another suggested that 'civil servants don't destroy anything' and DWP was no exception.

Providing training

The KIRM team provides training in IM and RM on request and it is only partially included in induction. The quality of the training presentations we reviewed was good. For example, the Records Management Introduction gives an overview of what records are, why it is important, how DWP does this, the various roles involved and responsibilities of staff for record keeping. All staff should receive at least a basic level of KIM training as highlighted in section 6 of the Lord Chancellor's Code of Practice on the management of records issued under s46 of the Freedom of Information Act 2000.[1] DWP is a large department, distributed across many different sites and it would be unrealistic to expect a comparatively small KIRM team to provide 'face to face' training to all staff. A network of information representatives in the business could help to delivery this training/reinforce the learning (see Section 3.2). Training doesn't have to be face to face; telekits, video conferencing, e-learning and the intranet could also be employed to share expertise and knowledge and ensure that key messages are communicated. **See Recommendation 5**.

Training will be particularly crucial during the rollout of a new ERMS. The importance of the cultural side of a technology change should not be underestimated, as insufficient training and support is often a key factor in unsuccessful ERM implementations. DWP should ensure that rollout is accompanied by a programme of mandatory training on how to use the system, 'floor walking' and helplines. Again, information representatives in the business will be crucial to the successful delivery of a new ERMS. **See Recommendation 2**.

[1] http://www.justice.gov.uk/information-access-rights/foi-guidance-for-practitioners/code-of-practice

All staff we spoke to knew about the Responsible for Information online training and why it was important and had attended this as required. Figures show that in 2014 around 71% of staff completed and passed the training.

3.4 Measuring impact

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

There are relatively few formal measures in place at present to measure compliance with the RM policy. A question on RM has been included in the Information Asset Assurance Returns and business areas are expected to provide evidence to demonstrate how they are meeting policy. This approach is still maturing and further detail could be given about what sort of evidence business areas needs to provide. (see Section 1 and Recommendation 5). The KIRM team also carry out twice-yearly file audits where 400+ registries are asked to provide lists of the registered files that they hold. If problems are found then these are escalated back up the management chain. DWP should explore the possibility of extending these audits to cover digital information on the shared drives (see Section 4 and **Recommendation 5**).

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.

Position of the DRO

The Departmental Records Officer (DRO) heads up the Knowledge Information and Records Management (KIRM) team which consists of seven people (including the DRO). Priorities are around creating RM policies, guidance and training, retention and disposal, selection, sensitivity review and transfer and overseeing the paper file audits. At present the review team is almost completely focussed on paper records and it is unclear how an increased role in managing digital information will impact on their work.

Oversight, control and use of records

The Department for Work and Pensions (DWP) transports, tracks and manages paper files on an almost unrivalled scale across government and the vast majority of this is customer information required for the process of delivering and administering benefits. DWP holds 57 million paper files and around four million of these are 'non-customer' files. There are two main paper stores at Heywood and Darlington and the assessment team visited the main store at Heywood. Capita have managed this service for DWP since 2004. There are 2-300 Capita staff on site at Heywood. The KIRM team has oversight of Capita's work – several members of the KIRM team are based on site at Heywood and work closely with Capita staff. Files are tracked using a digital system called Find and Retrieve Information Online (FARIO). Capita have a 99% success rate of being able to locate files. Non-customer files or 'DRO' files are kept separately at Heywood. This helps to ensure that material that needs to be reviewed is easily identifiable and helps the process of appraisal and selection run

smoothly. **This is good practice**. DWP are about to re-let the contract for storage and management of corporate and customer information records.

The KIRM team carry out twice-yearly file audits where over 400 registries are asked to provide lists of the registered files that they hold. These stopped for just under a year but were started again at the end of 2014. At present these only cover paper files. The KIRM team check these and if problems are found they are escalated back up the management chain. Issues found include registered files not being closed, registered files requested but not used and a general lack of registered files. It was estimated that of the returns received in the last audit, around 80% of these showed that the business areas were failing to manage their paper records in line with Knowledge and Information Management (KIM) guidance.

The lack of corporate system for Electronic Records Management (ERM) means that the oversight and control that the KIRM team has over paper records does not extend to digital. For example, they do not have oversight of the shared drives which are managed locally by business areas (see Section 2). DWP would benefit from extending the paper file audits to cover digital information, in particular that on the shared drives. **See Recommendation 5**.

Appraisal and selection

DWP has a team of four (three Records Management Advisors and a Reviewing Manager) that is responsible for the appraisal, selection, sensitivity review and preparation of files for transfer. The team work on all stages of the process rather than just one area which helps to ensure knowledge transfer. The team are experienced in appraisal and have built up a good knowledge of the history of DWP which helps them to make well-informed decisions on what to select for permanent preservation. There are clear criteria and guidance for reviewers on selection and DWP also has an Operational Selection Policy. The review team are employing macro appraisal techniques in line with The National Archives' guidance and where possible complete Series Level Appraisal Questionnaires (SLAQs) for file series in order to understand what type of records the series contains. Once these are

approved these are used to ‘sift’ out files of no value for destruction. They carry out spot checks to ensure that they are not getting rid of anything of value. The National Archives Information Management Consultant (IMC) has been able to approve reviews without need for regular rechecking. **This is good practice**.

Given that the organisation still runs a print to paper policy, there are no plans as of yet to appraise and select information held within shared drives. The shared drives are likely to contain information of corporate value that has not been printed off onto registered files. DWP therefore needs to engage with their IMC and begin to devise an approach for appraisal of information on the shared drives in order to identify material of historical value that should be transferred to The National Archives. Some of the macro techniques that it has applied to paper records can be adapted for this purpose. It should also consider how it will apply appraisal and selection to any new Electronic Records Management System (ERMS). DWP is a member of The National Archives Digital Transfer User Group and are therefore aware and able to learn from developments that other departments have made in the area of digital appraisal and digital transfer generally. **See Recommendation 6**.

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

DWP generally has robust and effective procedures in place for the disposal of paper files. Disposal information is added to the FARIO database for each file and Capita carry out disposal of paper files on a daily basis. This is doubly important due to pressure of space at the Heywood, particularly as they will be moving out of the Darlington store in the near future. There is a backlog on disposal of Human Resource (HR) records which is partly due to the outsourcing of some of the HR function and partly due to resource. However, the issue had been discussed with the DRO who was keen to find a solution.

Most of the benefits delivery systems have disposal built in although there are some omissions. The KIRM team is working with those areas to address this. DWP should ensure that all customer systems have a disposal function and that this is active. **See Recommendation 2**.

Disposal of digital 'non-customer' information is more ad hoc and is generally done at a local level, although central guidance on retention periods is available. For example, business areas are responsible for disposal from shared drives and email inboxes and users can delete posted information from Yammer. Although we found evidence to suggest that some areas do this well, overall practice was found to be inconsistent. Some interviewees reported that they regularly deleted records that they no longer needed but many did not. There is a risk that key corporate information could be lost through uncontrolled disposal or, on the other hand, that DWP is keeping too much information. DWP should consider extending the paper files audits to digital information and as part of this ask business areas to report on disposal. **See Recommendation 5**.

Sensitivity review

Sensitivity issues for DWP are relatively straightforward in comparison to other government departments in that they largely centre around sensitive personal information. The review team is responsible for sensitivity review and takes a decision on whether to close or redact depending on how much sensitive information is in a file. For example if there is a lot of sensitive information that would require a large amount of redaction, they will apply to close the whole file. If there is a small amount of sensitive information (usually an individual's name) they will redact and close this information and open the rest of the file. DWP's closure applications to the Lord Chancellor's Advisory Council are generally good and are approved without queries. DWP has not yet considered how it will sensitivity review digital information and needs to start developing an approach to this. **See Recommendation 6**.

Transfer and planning

DWP is currently ahead of target in terms of working towards the new 20-year transfer rule and they have no legacy backlog, as demonstrated by the Records Transfer Return figures for autumn 2014. It has a plan for review and knows exactly what it needs to review and when it needs to have been transferred. It runs a 'conveyor belt', systematic process of appraisal, sensitivity review, cataloguing, preparation and transfer. It currently has a large number of boxes awaiting cataloguing and preparation checks from The National Archives which is having a knock on effect on the space it has in order to start working on the next batch of files. There were some issues with the standards of cataloguing and preparation with the last batch of files transferred to The National Archives which led to a significant amount of re-work and as a result The National Archives checks are taking longer this time round. The KIRM team is fully engaged with The National Archives on these issues and are exploring a resolution.