The National Archives

Information Management Assessment

Home Office

Reviewed

June/July 2015

Published

May 2016

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 9

Recommendations to address risk areas 11

1 The value of information 15

2 Information and supporting technology 26

3 Information risk, governance and oversight 33

4 Records, review and transfer 45

Statement of commitment

In advance of each Information Management Assessment (IMA) we recommend that permanent secretaries publish a statement of commitment to the assessment process that also underlines the importance of good practice in information and records management. The Home Office has not published a statement of commitment. However, the department ensured that all participating units were made aware of their permanent secretary's commitment to the IMA process and to working with us.

IMA background

The Home Office IMA involved a detailed review of supporting documentation followed by interviews with senior staff, specialists and practitioners in the department's London office. These were conducted between 24 and 28 June 2015. Additional interviews with key staff were conducted at Heathrow Terminal 5 and by telephone into July 2015.

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:
nationalarchives.gov.uk/information-management/our-services/ima-reports-action-plans.htm

Glossary

CFP – Corporate File Plan

DRO – Departmental Records Officer

EDRM – Electronic Document and Records Management

EMB – Executive Management Board

FOI – Freedom of Information

HMPO – HM Passport Office

IAO – Information Asset Owner

IICSA - the Independent Inquiry into Child Sexual Abuse

IMA – Information Management Assessment

IT – Information Technology

KIEG – Knowledge and Information Executive Group

KIM – Knowledge and Information Management

KIMU – Knowledge and Information Management Unit

One3M – Home Office's information management and information assurance maturity model (previously I3M)

OSCT – Office for Security and Counter Terrorism

RMsys – Records Management System for tracking corporate paper records

SIRO – Senior Information Risk Owner

UKBA – UK Borders Agency

UKVI – UK Visas and Immigration

Key findings of the assessment

1 The value of information

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

- The Home Office is currently placing an increased priority on information and records management in response to well-publicised shortcomings that have had a negative reputational impact. We gained a good level of assurance that the Home Office is actively working to improve its ability to manage its records in all formats. The permanent secretary has been supportive, for example, giving his backing to the establishment of a new governance body. The department has also committed to developing a new information strategy. To deliver most benefit, we recommend that this should establish a joint approach for information and data. The Home Office has already identified as objectives through its risk management framework the principles of information availability, information security and information exploitation. These principles should be at the heart of the Home Office's new information strategy.
- The Home Office is working to increase oversight of its information assets and has undertaken Information Asset Owner (IAO) training, delivered by The National Archives' Information Assurance and Cyber Security Engagement Programme. However, there is not yet a single governance approach for the management of information assets, with HM Passport Office (HMPO) still maintaining its own separate processes. Internally published guidance for IAOs is generic rather than specific to the Home Office and is unlikely to be providing effective direction to staff. The Home Office needs to clarify whether its open and inclusive definition of an information asset should routinely be applied to unstructured information. It should also more clearly establish the extent to which the concepts of records and information assets overlap. Records management and information assurance staff should work together to ensure that retention requirements are identified for existing information assets.

2 Digital information and supporting technology

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

- The Corporate File Plan (CFP) meets key requirements of the Section 46 Code of Practice but is inflexible and under-used. The introduction of the SharePoint 2010-based system, iManage, is expected to help the Home Office manage its digital information more effectively, making information easier to find and reducing the burden on users.
- The introduction of iManage has been formally identified as a mitigating action for the information availability related risks that the Home Office faces. The Home Office needs to ensure alternative mitigating actions are also defined for areas where the CFP is not in use and where iManage will not be adopted. This includes areas such as the Office for Security and Counter Terrorism (OSCT), which is upgrading from SharePoint 2007 to SharePoint 2013. To effectively manage these risks and help ensure the success of its new system, the Home Office must also address the significant volume of information held outside shared repositories in email accounts and personal drives. These lack size limits or auto-deletion functionality that may have been helpful in encouraging staff to store emails in corporate repositories.
- The Home Office has good foundations in place to support the management of digital continuity risk, but lacks formal plans to enable this. It should embed its approach in its new strategy and include a description of digital continuity risk at a proportionate level in its risk management framework, engaging with its IT supplier as needed. This is particularly important in view of the length of time that some of the Home Office’s information and data will need to be maintained.

3 Information risk, governance and oversight

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

- Risks relating to information exploitation, information security and information availability are defined at appropriate levels in the Home Office risk management framework. Risks are well described. The information availability risk is owned by Corporate Services. It establishes the impact of poor performance in information management and the role of KIM improvement work in reducing the risk that the Home Office faces. Current risk descriptions do not make reference among mitigating actions either to steps taken by the business to adhere to policy or to central compliance checking activities. Both points should be addressed at an appropriate level within the Home Office risk management framework. The Home Office should also assess whether it is gaining the insight it needs into work to reduce information availability risk across all areas of the business, with particular reference to areas where KIM governance is not delivered by the Corporate Services based Knowledge and Information Management Unit (KIMU).
- We strongly support the creation of the Knowledge and Information Executive Group (KIEG), which has the potential to provide a new impetus to work to improve information management standards. The Home Office also needs to resolve the way responsibility for information and records management governance is distributed across its groups. In our view, arrangements at the time of the IMA, with responsibility divided between separate knowledge and information management teams, did not yet reflect the Home Office's status as an integrated single department. The Home Office needs to work to deliver a more consistent governance approach. The KIEG has the potential to play a key part in this.
- The Home Office recognises the need to improve the quality of guidance it

provides to staff. Work to review and improve this was underway at the time of the IMA. We support the Home Office's aim of adopting a three-tier approach with detailed policy that is accompanied by guidance and briefer desk guides. In particular, staff need clearer guidance to help them recognise what to keep. With this in place, it will be easier to encourage greater business ownership of information and records management.

- Capability in information assurance and information management is assessed at group level via the Home Office One3M maturity model. We recognise this as a useful means of benchmarking performance. The model is based on the 2012 HMG Information Principles and has evolved to test performance in new priority areas such as cyber security. The Home Office should now review the basis on which the model is established as adherence to the information principles is no longer mandatory. At the same time, it should consider shifting the focus of the model to deliver a more in-depth, qualitative assessment of whether policy and guidance are being adhered to.

4 Records, review and transfer

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

- The Home Office Departmental Records Officer (DRO) is also the Head of KIM and is well placed to oversee paper and digital as a whole. The DRO is in a good position to exert strategic influence and ensure that the potential impacts of information and records management related risks are clearly communicated. The Home Office recognises the limitations of its tracking system for corporate paper records, RMSys. It has conducted a data cleansing project to improve the quality of data on the system before a replacement is implemented; an audit of paper files held by the business was also commissioned by the permanent secretary in support of the review carried out by Peter Wanless and Richard Whittam QC. The department has conducted specific digital searches in response to the Rotherham child sex abuse investigations and this has led to a wider piece of work aimed at improving eDiscovery.

- The Home Office continues with appraisal work, with a view to ensuring it can get back on track with the preparation and transfer of files to The National Archives. It has published its disposal schedules in response to recommendations in Sir Alex Allan's Records Review report.[1] It is also an active participant in The National Archives' Digital Transfer User Group. At the time of assessment, disposal of records was on hold in accordance with the requirements of the Independent Inquiry into Child Sexual Abuse (IICSA). With reduced resources following a KIM team restructure, the Home Office needs to produce a revised forward plan for the appraisal, sensitivity review and transfer of its records. It also needs to have clear criteria for the disposal of information not migrated to iManage, and should work to improve its knowledge of the information stored in its unstructured shared drives.

[1] www.gov.uk/government/publications/records-review-by-sir-alex-allan

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 2015 IMA
The need to improve information and records management has been communicated at the most senior level within the Home Office and the backing of the permanent secretary has been obtained for key initiatives. These include the establishment of a Knowledge and Information Executive Group to help deliver better governance and senior engagement.
The previous information strategy, though now lapsed, delivered tangible outputs and was prominently endorsed by the then Senior Information Risk Owner (SIRO).
The Home Office has invested effort in improving its performance in responding to enquiries under the Freedom of Information (FOI) act. Weekly performance targets are in place, with weekly meetings used to flag any issues. The Home Office has published the highest volume of FOI releases of any department of state on GOV.UK – 1,674 of the 4,798 documents published by the department (as of 1 June 2015).
A requirement has been established to consider transparency as a factor in business cases over a specific threshold, and the Head of Transparency sits on the project boards of larger projects.
By defining a strategic-level risk relating to information exploitation, the Home Office has demonstrated that it recognises the true value of its information and the impact if this information cannot be used as needed.
The Home Office has described an information availability risk that includes a range of cultural and IT-related causes. The risk description clearly establishes the impact of poor performance in information and records management for the department and establishes the role of KIM initiatives in

reducing the level of risk that it faces. Undergoing an Information Management Assessment has been included among mitigating actions in recognition of the benefit that can be obtained from external scrutiny and review.
A Service Level Agreement is in place for knowledge and information management, which sets out responsibilities of the central team and the business.
Results from assessments using the department's information management and information assurance maturity model (One3M) are shared with internal audit and help inform audit plans for the coming year. Consolidated results are shared with the SIRO.
A Historical Inquiries and Review team has been set up to handle all e-discovery work with the exception of FOI. This team has been engaged with the Independent Inquiry into Child Sexual Abuse (IICSA) from the start.

Recommendations to address risk areas

Recommendation 1

The Home Office should build on its KIM action plan and ensure that the new information strategy owned by the Knowledge and Information Executive Group (KIEG) sets goals for the whole department. The strategy should provide an impetus for work to improve technology, governance and culture.

There would be benefit in centring the strategy on the principles of information availability, security and exploitation that are already defined as objectives in the department's risk governance approach.

This would be supported by:

- Establishing a joint or linked strategy for corporate information and data to tackle the current siloed approach.
- Factoring in plans to increase oversight and control of operational records.
- Factoring in digital continuity considerations and defining a digital continuity risk at an appropriate level (such as the performance and risk directorate risk register).
- Underlining the benefit the adoption of the information strategy will deliver to the department with endorsement by the Senior Information Risk Owner (SIRO) or at Executive Management Board (EMB) level.
- Establishing a requirement to report to EMB or SIRO at appropriate milestones.

Recommendation 2

KIMU and information assurance staff should work together to increase oversight and control of the Home Office's information assets, establishing clearer department-specific principles for Information Asset Owners (IAOs).

This would be supported by:

- Defining more clearly the relationship between records and information assets.
- Ensuring that retention requirements for existing information assets are visible to the Departmental Records Officer (DRO).
- Bringing greater consistency to the IAO role and establishing how IAOs should be supported in provision of assurance (for example, by a specific role or by their teams).
- Reviewing the IAO handbook to reflect the processes in place within the department

Recommendation 3

Develop plans to increase oversight and drive good governance of the information held outside the Corporate File Plan (CFP) and iManage, information not migrated to iManage, and the information held in personal repositories and unstructured shared drives.

This would be supported by:

- Identifying who has responsibility for governance of unstructured shared drives (see also recommendation 4).
- Defining an approach to address and limit the storage by staff of important information and ephemera in email accounts in the future.[2]
- Defining an approach to ensure the availability of information with long-term historical or business value currently held in email accounts and shared drives (see also recommendation 5).[3]
- Ensuring that information not migrated to iManage becomes read-only and that a plan is in place for its disposal. Where information has long-term value its continuity will need to be maintained.
- Defining the mitigating actions for information availability risk in those areas where iManage will not be adopted and where the CFP is not in use.

Recommendation 4

Establish a single approach for knowledge and information management governance that cuts across the existing group structure to drive consistent, department-wide improvement.

This would be supported by:

- Establishing more formal links between the DRO and head of KIMU, IMCU and OSCT. KIM teams should support the effective planning and delivery of the new information strategy.
- KIEG endorsement of key documents that set out KIM functions and roles (such as the Terms of Reference for the Home Office Head of Knowledge & Information Management Profession and the KIM service level agreement) to provide a basis to hold the business and KIM staff to account.

[2] The National Archives' guidance recommends imposing size limits on personal repositories and email accounts as a means of encouraging corporate storage of information with value. The Home Office should consider this in the future as part of wider plans.

[3] The Home Office should also recognise the limitations in terms of time available to staff as well as the potential impact of users transferring large amounts of email at once, learning from the experience of other government departments.

- Ensuring that consistent branding and common principles are applied to KIM policy.
- Ensuring that monitoring of information availability risk, and progress made in addressing it, cuts across group boundaries

Recommendation 5

Establish a plan to ensure messages about information and records management requirements and responsibilities are reaching all staff across all groups.

This would be supported by:

- Seeking KIEG sponsorship and the support of senior management for this work.
- Extending the responsibilities of business areas and managers (as set out in documentation such as the KIM service level agreement and *Managing information: manager's responsibilities*) to include ensuring that staff adhere to information management policy.
- Using One3M (or other means) to make qualitative assessments of the extent to which policy and guidance is being followed. This may form part of wider work to review the basis on which the model is established.
- Publicising One3M results internally to raise standards.
- Considering obtaining assurance from the business at an appropriate level that information is being kept as required against defined standards. This may help embed understanding of corporate responsibilities.
- Ensuring the business owns the risk of not taking the right action to adhere to information management policy. This risk may, for example, be defined and owned at group or team level. Action taken to monitor compliance should also feature in central risk descriptions.
- Reviewing and improving training and guidance provision: in particular, looking at developing bite-size guidance and use of e-learning.
- Reviewing the provision of information support roles to better fit the Home Office's needs. This might include, for example, splitting the iManager role into two, with one role focusing on oversight and promoting good KIM practice while the other focuses on more administrative tasks.

Recommendation 6

Establish a plan for achieving 20-year rule commitments for the remainder of the transition period, ensuring that a clear process and guidance for review staff are defined.

This would be supported by:

- Producing a revised forward plan for the appraisal and transfer of records, in all formats, which factors in quality requirements and available resources.
- Considering the reduced team size, reviewing sensitivity review guidance to ensure that as much information will be released as possible and sensitive information will be protected where possible.
- Continuing to investigate macro methods of appraisal.
- Continuing to work alongside The National Archives in developing a process for appraisal, sensitivity review and transfer of digital information, drawing on the experience of other government departments and its own Information Management Consultant.

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 Home Office has been subject to criticism and reputational damage because of its inability to demonstrate that it could locate information relating to historic child abuse allegations. The 2014 review by Peter Wanless and Richard Whittam QC was set up to examine whether the Home Office had failed to act in the 1980s on information it received in respect to allegations of organised child abuse involving public figures. Their review highlighted gaps in filing conventions and record keeping methods. Because of these gaps, the authors concluded that it was 'not possible to say whether files were ever removed or destroyed to cover up or hide allegations of organised or systematic child abuse'.[4]

In response, the Home Office has publicly committed to improving processes for discovery of existing paper files.[5] This is to be achieved through better housekeeping of files and replacement of the department's paper record system, RMSys, as recommended by one of two recent Home Office internal audit reports that looked at information and records (see p.24 and 46).

Through our assessment, we saw evidence that the Home Office is also giving priority to the management of current digital information and to ensuring that the right records are created in the first place. A new KIM team is in place under a Senior Civil Service-level Departmental Records Officer (DRO) and support has been sought

[4] The Wanless and Whittam QC review: www.gov.uk/government/uploads/system/uploads/attachment_data/file/372915/Wanless-Whittam_Review_Report.pdf

[5] Annual report and accounts 2014-15: www.gov.uk/government/uploads/system/uploads/attachment_data/file/441282/HO-AR15_web.pdf

from the department’s permanent secretary to take action to improve performance in the following four priority areas:

- Improved understanding
- Better technology
- Better control
- More reward and recognition

We recognise these as appropriate areas to target and are pleased to see that the first steps have been taken, with a letter sent to Executive Management Board (EMB) members seeking engagement on the formation of a new KIM governance board, the Knowledge and Information Executive Group (KIEG). The Home Office used this opportunity to emphasise to EMB members the role of information as an enabler for the department’s public task. The letter also stated that leaders within business units need to take responsibility for the way their staff manage knowledge and information.

Policy and guidance already contain some helpful messages on the importance of good information management and staff obligations in this regard. For example, the information management home page on the Home Office intranet, Horizon, provides the following clear statement:

> *Every civil servant is responsible for managing the information and documents they create and use in their work. It’s a requirement of the civil service code that we: ‘keep accurate official records and handle information as openly as possible within the legal framework’*

However, from our interviews it is clear that such messages are not being heard or recognised by all staff. Across the department as a whole, staff awareness of records management as something that matters to the Home Office was varied. In 2013, the Home Office took on responsibility for the functions of UK Border Agency (UKBA) and the executive agency status of HM Passport Office (HMPO) was removed in 2014. A substantial number of the staff who are now Home Office employees fulfil frontline roles and are based outside the corporate centre. In our view, staff interviewed from these areas in particular tended to be less clear about corporate messages relating to information and records management.

A push on records management responsibilities is something that a number of the staff we spoke to actively want their department to provide. Several interviewees expressed the view that the Home Office needs to make it clearer that everyone has a responsibility to manage their information. One felt that the Home Office needs ‘to push harder on the fact that everyone has responsibility for IM, with a commitment to support this by providing better systems.’ Another stated, ‘Everyone has responsibility for RM, but it is particularly important for managers and particularly important to convey to new staff. Staff need to get the message that this is business critical.’ A third staff member said, ‘Policy and strategy for IM is not embedded in the culture … Home Office needs to drive policy to individuals and build it into people’s roles and get people to do the right thing. If this had happened all along the department wouldn’t be having the problems it is having now in terms of responding to inquiries. The longer Home Office takes to address it, the bigger the problem will be.’

Key messages about information and records management must reach all staff. Leadership from senior management would be helpful in ensuring these messages are heard and understood across the whole department. We recommend that a specific plan is established to ensure that they are communicated effectively. It is worth noting here that Horizon has not proved a successful tool for this so far – staff we spoke to outside the corporate centre said they found it very difficult to search and that it was often slow. The continued rollout of the department’s new SharePoint system, iManage (see pp. 27-8), may offer at least part of the solution. It has the potential to provide a shared corporate storage area and a tool for communicating messages about good practice in records and information management. It is also expected to help staff communicate better across team boundaries. In addition, the Home Office should make greater use of its networks of Records Advisors and iManagers to promote KIM messages. **See recommendation 5**

Setting goals for information and its management

In 2012, the Home Office 2010 information management strategy, *Want to know more?*, was refreshed and reissued under the title *Still want to know more…?* Although not time bound and lacking a schedule for further review, the strategy was endorsed by the then Senior Information Risk Owner (SIRO). **This is good practice**. We also note that the strategy provided impetus for the development of tangible outputs in the form of the Home Office's I3M maturity model (see pp. 42-4). This was introduced to provide a framework for an evidence-based assessment of Home Office policies, procedures and practices against the HM Government Information Principles.

Still want to know more? has not been revisited or revised recently – for example, since the incorporation of the former UKBA or HMPO into the Home Office – and it is no longer a live document. We are, therefore, pleased to note a commitment from the Home Office to develop a new strategy, following the publication of this report, that will be owned and taken forward by the KIEG.

In the absence of a current information strategy, we highlight the existence of two separate action plans that are providing direction: the Home Office Data Science action plan and the Improving Knowledge and Information Management in the Home Office action plan. The former sets expectations for the deployment of data science, capability development and work to overcome barriers. A key goal is the establishment of a single data platform under the direction of the Home Office Data Analytics Capability to 'unlock the value of data in Line of Business systems'. A data board has been formed and a programme is in place to migrate data and decommission five existing systems. Benefits highlighted by interviewees include a shift from a case-focused approach to a more holistic person-focused approach for the data the Home Office collects on individuals, with the ability to establish a 'customer' narrative. We understand that the establishment of a data directory will form part of this work.

Meanwhile, the Improving Knowledge and Information Management in the Home Office action plan sets out necessary steps to address performance in historical search and review and in the four priority areas for improvement that have been highlighted to the permanent secretary (see pp. 15-16). The Improving KIM action plan provides a clear summary of the issues that need to be addressed. We regard the development of this document as a useful start in developing a targeted approach, but note that it is not time bound, corporately branded or endorsed. It does not set out how actions will be delivered, or who will be responsible for delivering them over what period.

The central Knowledge and Information Management Unit (KIMU) sits within Corporate Services. The Office for Security and Counter-Terrorism (OSCT) has its own KIM team, while Immigration Enforcement, UK Visas and Immigration (UKVI) and Border Force are managed through the Information Management & Compliance Unit (IMCU). These sit in different business areas from KIMU and are working to different corporate requirements. KIMU has drafted its 2015-16 business plan according to Corporate Services principles. The schedule of work within this document, while not mapping precisely to the Improving KIM action plan, clearly covers a number of its priority areas. IMCU lacks a direct senior civil service chain and has not produced a 2015-16 business plan. Meanwhile, OSCT staff are working to deliver their own, separate KIM strategy from 2010. Because of this, and because of the lack of reference in the Improving KIM action plan to specific challenges within OSCT, Immigration Enforcement, UKVI and Border Force, it is not clear how far the document applies to them in practice. To drive consistent improvement and risk mitigation, the Home Office needs to ensure that planned work applies to the whole department. The information strategy it develops must set goals that enable this. **See recommendation 1**

A number of senior staff interviewed were open to the idea of a joint strategy covering information and data. Similar goals are already being set for information and data in terms of ensuring that they are available to meet business needs, and are supported by effective technology. Datasets, like unstructured information, have lifecycles that need to be managed and some will need to be maintained for a considerable length of time. We also note that, from a risk management point of view, the Home Office already has a joined-up approach, with strategic risks relating to information exploitation defined in an inclusive manner that covers information and data.

As the Home Office has already defined information security, information availability and information exploitation (see p. 33) as objectives through its risk management framework, we recommend that it establishes these as the core principles for its new information strategy. We recommend that the Home Office should either establish a joint overall strategy for its information and data, or ensure that individual strategies and plans are formally linked and structured around these common principles. **See recommendation 1**

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

According to the latest published statistics for FOI at the time of the IMA (Q4 2014), the Home Office received the fifth highest number of FOI requests (692) among the departments of state.[6] This is itself the lowest volume that the Home Office has received since Q3 2012. 80% of requests in Q4 2014 were met within the 20-day deadline and 90% were answered in time (in other words, meeting deadline or within permitted extensions). Home Office response rates dipped below 85% in Q3 2012 and remained below this level through 2013. We were told that this was due, in part, to structural changes and loss of expertise during the transfer of the former UKBA's functions to the Home Office. The Information Commissioner's Office monitored the Home Office's timeliness in responding to requests for information between July and September 2013. The Home Office's performance improved in 2014 and remained above the required level in three out of four quarters. It granted 38% of resolvable queries in full in Q4 2014, which was below the average of 49% for departments of state. It also withheld in full 39% of resolvable requests, which was above the average of 32% for departments of state.

Interviewees indicated that there is now very close scrutiny of the FOI process and performance within the Home Office, with regular reporting to senior staff. Current FOI processes appear to be robust and were recognised as such by interviewees. The Information Rights team operates a partially devolved service, handling around a third of FOI requests directly and providing a coordinating role for the remaining requests. These are dealt with by Information Access practitioners in the business.

[6] www.gov.uk/government/collections/government-foi-statistics

FOI guidance has been recently refreshed and the team has put in place weekly targets and uses weekly meetings to flag anything problematic.

As at 1 June 2015, there were 4,798 publications by the Home Office on GOV.UK, 306 of which were classed as transparency data. The department has published 284 datasets on data.gov.uk. The website gives the department an average score for openness of 1.7 and it has received a total of 483 stars, the third highest number among departments of state. Key successes noted by interviewees included making places of worship data available in open data format and the provision of data that underpins the police.uk website. The Home Office has also recently published the raw data for that website. We were told that a requirement has been established to consider transparency requirements in business cases over a certain threshold. The Head of Transparency sits on the board for larger projects with links in to digital and open standards work. **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

The Home Office has a main information asset register for logging significant information assets, with a threshold for inclusion based on factors including sensitivity and business criticality. Information Asset Owners (IAOs) should log information assets that fall below the threshold for inclusion on local information asset registers. We understand that a suggested template is provided that includes 14 fields.

The Home Office IAO Handbook sets expectations for the management of information assets in the department. It defines an information asset as:

> *A body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively.*

This is the standard government definition, promoted through supporting documentation for the security policy framework and by The National Archives.[7]

The Home Office IAO handbook contains many positive elements. These include a clear definition of the risks that information assets may be subject to, such as cyber security and information management related risk. The Home Office worked with Cabinet Office to produce this document, which was drafted in a generic style with the hope that other government departments would be able to make use of it and adapt it to reflect their own business needs.

We recognise the IAO Handbook itself as a best-practice template, but it can only have limited utility as a piece of guidance if it is not tailored. The Home Office has not done this when publishing the handbook internally and has made the guidance available to staff in its generic form. The handbook states throughout what 'your organisation' or an IAO within 'your organisation', should do. It does not set out how processes actually work in the Home Office or particular groups within the Home Office, or what the specific expectations are for the Home Office's own IAOs. Governance arrangements are not established and the department's name does not feature within the branding or contents. In addition, while the handbook contains links to guidance published by the Information Commissioner's Office and The National Archives, it does not link to any internal Home Office policies covering areas such as information security, information assurance or information management.

The Home Office's approach for identifying and maintaining oversight of its information assets is still evolving. A project was run in 2014 to bring the main information asset register up-to-date and identify and include information assets held within the former UKBA. The project did not extend to HMPO, which still oversees its own information assets and maintains its own assurance process. This means that the Home Office does not yet have a single structure for the management of its information assets.

We found evidence that the concept of an information asset is not yet fully embedded and that information assets do not yet appear to be consistently identified

[7] www.gov.uk/government/publications/information-asset-owner-role-guidance

and logged. In one case, we carried out a spot check on an information asset that contained sensitive information with long-term business value and that had been subject to digital continuity loss earlier in its life. The information asset in question did not appear on the main information asset register at the time, but was subsequently added, confirming our view that it had been over the threshold for inclusion. In other cases, staff we interviewed were unclear why particular bodies of information they described to us would be classed as information assets and logged on local information asset registers, although they met criteria set out in the IAO Handbook.

In particular, we saw limited evidence that the definition of an information asset was being routinely applied to proportionate groups of unstructured information and records, as set out in the IAO Handbook. Not all directorates had included examples of this type of asset on the information asset register extract supplied to us for review. Exceptions included one directorate that had catalogued information assets described as containing draft and finalised reports and advice given on specific topics. While the IAO Handbook specifically states that all files associated with a project may be classed as an information asset, only the HR directorate had listed information assets containing project documentation. We also noted that Home Office guidance on project management makes no reference to the concept of information assets, IAOs or to the processes that should be followed.

One underlying cause may be the fact that the Home Office has not fully established how the concepts of records management and information asset management overlap and support each other. Of particular interest from the point of view of this report is the lack of clarity around oversight of retention requirements for information assets. The main information asset register has a column to collect retention requirements with a heading indicating that these should be passed on to records management staff, but this is not happening. Within HMPO, retention requirements are not collected at all.

This is concerning because, in practice, everything that government departments generate is a public record and needs to be managed as such. Departments have a responsibility under the Public Records Act to ensure the safekeeping of everything they generate, whether or not it will ultimately be identified as having historic value and selected for permanent preservation.[8] Risks relating to the future availability of information assets may be increased if retention requirements are not identified or are not applied correctly. The DRO and SIRO need assurance that the right criteria have been identified for the retention of the Home Office's information assets. We recommend that the Home Office tightens its procedures in this area and ensures that retention requirements for information assets are subject to more effective scrutiny with closer involvement from the DRO and his team. At the same time, it needs to amend the IAO Handbook to establish department-specific principles and provide clear direction for its IAOs. This should include clarifying the relationship between information assets and records. **See recommendation 2**

Ownership of information assets

We recognise that the Home Office has been working to address understanding and visibility of the IAO role. We are pleased to see that the Home Office has taken advantage of IAO training provided by The National Archives' Information Assurance and Cyber Security Engagement Programme, with just under 200 IAOs from across the department trained through to March 2015.

The Home Office does not appoint its IAOs at a specific level of seniority, but there is an expectation that staff with more seniority will have responsibility for more significant or sensitive information assets. IAOs with less seniority should escalate usage requests for smaller information assets such as extracts from larger datasets. In contrast to a number of other departments, the Home Office does not nominate any specific support role to help IAOs discharge their duties or define how certain responsibilities may be delegated in practice. The Home Office should consider doing this - for example, to establish responsibility for the day-to-day management of larger information assets. **See recommendation 2**

A number of the issues we encountered were identified in the 2014 Home Office internal audit report on information assurance. It is clear to us that much remains to be done to bring consistency to the role of IAO and to ensure that it delivers benefit

[8] The Public Records Act: nationalarchives.gov.uk/information-management/legislation/public-records-act/

to the department. We recommend that a specific plan is put in place to improve oversight of information assets with involvement from KIMU and information assurance staff. This is particularly important given the Home Office’s aspiration to utilise new opportunities offered by iManage to delegate more responsibility for information asset management to local teams. **See recommendation 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 core Home Office has had a main repository for unstructured information since the introduction of the Corporate File Plan (CFP) in 2005. The Home Office has invested considerable effort in maintaining the CFP, which is functionally based and has a documents and records area. The latter offers the ability to manage information and protect records from accidental or unauthorised alteration, copying, movement or deletion in line with guidance set out in the Section 46 Code of Practice.[9] A number of interviewees stated that the CFP met their needs at a basic level, with one describing it as 'a solution to a problem, but old-fashioned'. The CFP has some key limitations and the Home Office recognises that these have had a negative impact on buy-in to and use of the system. KPIs are in place for the creation of folders, which the Home Office reports are always met or exceeded. Despite this, there was still a perception among some staff we spoke to that processes for setting up files can be time consuming, that the structure is inflexible or hard to change, and that in some cases it has not been kept up to date effectively as needed. Others questioned how well the CFP is adopted and used, saying: 'Even where CFP has been embraced, practice isn't consistent,' and 'A lack of naming conventions means you can't find anything if there are large numbers of files in a folder'.

The Home Office hopes to address the limitations of the CFP through the introduction of iManage, which is based on SharePoint 2010 and is intended to lessen the burden on staff. Within the current technology environment, however, matters are complicated by the fact that the CFP has not been available to the whole

[9] The Section 46 Code of Practice: www.nationalarchives.gov.uk/information-management/manage-information/planning/records-management-code/.

department. This means that the Home Office is not starting from a level playing field, with some areas facing greater or lesser risks in information and records management terms.

For example, OSCT has its own SharePoint 2007 implementation, with a Meridio bolt-on that supports records declaration, but not disposal. This has historically been delivered by a different IT supplier to that used by the rest of the department. Border Force, meanwhile, and other areas that formed part of UKBA, use unstructured shared drives. These are not subject to central oversight or control and do not offer the same benefits as the CFP in terms of the lifecycle management and protection of information from unauthorised alteration, copying, movement or deletion. We saw evidence of the potential impact of this from a business perspective. In one case, we were told that a dataset identified by interviewees as having significant current value to the Home Office from a reporting point of view had been inadvertently deleted and staff had to contact IT to try to retrieve it.

We note that a print-to-paper policy is in place for Border Force’s key operational outputs. This could help reduce some of the risks that the current provision and use of this environment raises to information with long-term historic value, as long as the policy has been and is fully adhered to.

Electronic Records Management System - iManage

iManage is being consciously adopted as a ‘stop gap’ solution to improve the Home Office’s information and records management performance ahead of the department’s move to a new technology platform by 2017.

iManage is the Home Office’s name for the EDRM software procured as a service from its IT supplier, Fujitsu Cloud Services. It is being rolled out with an Automated Intelligence Compliance Extender to boost the records management functionality and Automated Intelligence Syncpoint to enable email integration. We were told that the Home Office will no longer be relying on users to create metadata, close files or declare records, as much of this will now be automated. The system has the capability to manage information through its lifecycle and has so far been rolled out to around 3,500 staff, with plans to roll it out to another 9,000 in autumn 2016. The CFP was still in active use at the time of the IMA and requests to set up new folders were still being made. We understand that the CFP is being progressively shut down from January 2016.

There is no plan yet to remove access to alternative storage areas, such as shared and personal drives and the CFP, once iManage is fully up and running, although some business areas have already asked KIMU to do this for them. If staff continue to have access to alternative repositories when iManage has been rolled out to them, there is a risk that information with value will be stored outside the system, undermining the expected benefit to be obtained from its introduction. Access to these alternative filing areas should be removed once iManage has been fully rolled out, staff are aware how to use the system, and any important information has been migrated across to it. **See recommendation 3**

Finding, accessing and protecting information

The way that digital information has been managed within the Home Office has led to substantial issues around its discovery. As one member of staff commented, these have 'exposed the risk - the causes of which are a lot of data and versions and poor understanding of what should and should not be stored.' The introduction of iManage is expected to help address this and make it easier to find information stored in shared spaces. This has been a key driver for the push to adopt iManage.

While this is positive, we note that iManage is listed as the sole IT-related mitigating action for the information availability risk that the Home Office has identified (see p. 33); it is also the sole IT-related solution for shared storage areas listed in the Home Office Improving KIM action plan (see pp. 18-19). At the time of the IMA, it was not clear how far the system would be rolled to the operational areas of the Home Office and what the benefits there would be. As noted elsewhere in the report, these are areas of the Home Office where there have been gaps in provision and awareness of information management policy and where unstructured shared drives are in use rather than the CFP. Both factors are likely to increase the risk that the information the Home Office needs will not be available. The Home Office should ensure that alternative mitigating actions are clearly defined and communicated for areas where iManage will not be adopted. This includes OSCT and any areas where unstructured shared drives will continue to be used. **See recommendation 3**

The Home Office has also identified the storage of information in personal repositories as a concern. While there is an aspiration to address this through the 'better technology' component of the Improving Knowledge and Information Management action plan, as yet there is no concrete plan to do so.

The Home Office provided us with approximate estimates that around 50 TB of information is held in individual and shared mailboxes and 30 TB is held in personal drives. There are no limits on email storage across the whole of the Home Office and no limits on the size of personal drives in the majority of the department. The exception is OSCT, where limits on personal drives are in place and interviewees highlighted an active policy of encouraging staff to file emails and keep inboxes to a reasonable size. A lack of limits makes it possible to hold large volumes of information that may have corporate value outside shared spaces. This may mean that information is either held for longer than it needs to be or disposed of prematurely when it should be retained. A number of interviewees stated that they saved emails into the CFP when they needed to record a decision or agreement. However, it was clear that other interviewees were retaining and managing large volumes of emails within Outlook folders. Some of the staff we spoke to reported inboxes with five, ten or more years' worth of email, including information from previous roles. To underline the scale of the problem, we also heard accounts of inboxes that had become unstable because of the volume of emails that had been retained in them.

One member of staff stated that they were unclear about the rules relating to retention, but never deleted emails and held large volumes to ensure they had a record of decisions 'because I've been burned in the past'. Another who similarly said they were holding a 'huge' amount of email and were unaware of corporate guidance said 'I don't delete anything in case I need to go back to it.' In one case an interviewee said that they kept emails for their own audit purposes, but applied their own retention policy, deleting everything over three years old on a rolling basis.

The Home Office has previously conducted deleted/junk email initiatives and has in the past planned to put hard limits in place for email accounts and personal drives, while at the same time encouraging and enabling storage in shared repositories. The Home Office has a network-accredited date-based retention tool that could, in theory, be applied to both areas to reduce the length of time information is held and the size of these areas. It is also considering the use of e-Discovery tools to help identify information with value held outside shared repositories.

The Home Office needs to identify and address information that is currently held in personal repositories, including email accounts, that should be retained and information without value that should not be. It also needs to address and limit the storage by staff of important information and ephemera in email accounts in the future. The Home Office does not now intend to impose limits on personal repositories within the current IT environment. We recommend, though, that it should consider doing so in the future as part of wider plans to address these issues. These plans should contain a significant cultural component. Any solution for information currently held in email accounts and personal drives needs to recognise business as well as historic value, and be practical and proportionate. Staff are unlikely to be able to spend extended periods of time reviewing old emails or documents to decide what should be kept. **See recommendation 3**

Plans also need to balance the requirement to engage staff and ensure that information with value is captured with the potential negative impact on iManage's stability if large volumes are moved in one go. The Home Office intends to mitigate the risks through guidance and training. It is recommended that the Home Office learns from the experiences of other departments using Syncpoint, such as the Department of Health - in particular, the impact on iManage if users start to transfer large amounts of email at once. **See recommendation 3**

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 type and format

It is relatively easy for the Home Office to understand the age and type of information that is held on the CFP and iManage, which are both subject to central control and oversight. This includes records from the department's old EDRM system, Meridio, which were created between 2005 and 2012. These were migrated to the CFP, but lost some metadata in the process. Date last modified has been retained.

As noted above, there is no central oversight of the shared drives inherited from the former UKBA and no central knowledge of the type, format or state of information held in them. Without such knowledge it will be harder for the Home Office to ensure its information remains accessible, readable and useable according to business need. We were told by interviewees that some of this information dates back to the early 1990s. The Home Office hopes that the use of e-Discovery tools will help it to address this.

In addition to this, the Home Office's historic data in case management environment is complex, with data management carried out on a system-by-system basis. Data has different structures, different retention, different mandatory fields and is of different quality. Although the Home Office is in the process of moving to a common data platform, the current state of data management has proved challenging in terms of responding to requests for information and investigation. This complexity and the challenges involved in maintaining usability underline the importance of establishing a joint strategy and a joint approach for ensuring the continuity of data and digital information. **See recommendation 1**

Digital continuity planning/IT change

We gained a good level of assurance that business requirements for information management are at the heart of plans to roll out iManage. OSCT are moving to a different version of SharePoint (2013). Interviewees indicated that differing solutions may be used for at least some aspects of these two projects: for example, iManage will utilise a records centre and OSCT will consider managing records in place. This is concerning as, without customisation, the latter approach may put stored information at risk of inadvertent deletion. However, it is positive to hear that OSCT has engaged and consulted with KIMU on key aspects including content types.

Although there is no joint approach for management of retention requirements for existing information assets, the DRO has good visibility of the ICT procurement process. As an assessor, the DRO has the ability to comment on and contribute to business cases. **This is good practice.** We were given verbal assurance that helpful informal links exist between IT and KIM staff, which should help ensure that iManage is factored into the Home Office's forthcoming IT refresh. The inclusion of IT subject matter experts alongside senior business representatives as standing members of the KIEG offers the opportunity to strengthen and formalise these links.

While the Home Office has solid foundations in place to ensure that digital continuity risks are managed, it does not yet have a plan to enable this. In addition, while it has a sound approach to documenting information risks in general as described below, we also note that it has not yet formally defined any risks in this specific area. The recommended joint approach for managing information and data should include managing their continuity. Information and data needs to remain usable through to disposal or transfer to The National Archives. The fact that the Home Office has large volumes of data that may have to be retained for anywhere from 50 to100 years makes the lack of policy structure around digital continuity a particular concern. **See recommendation 1 and 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 Home Office has defined a strategic-level risk relating to the exploitation of information. The Home Office is one of a small number of departments among those we have assessed to have done this. By defining this risk, the Home Office has demonstrated that it understands the value of the information that it works with and the potentially significant impact if this value it is not realised effectively. **This is good practice**.

Beneath the level of the main corporate risk register, the Corporate Services risk register contains a well-described risk relating to information loss. From an information security point of view, an appropriate range of potential causes have been identified, ranging from a failure to adhere to guidance, to insider threat and cyber-attack. In summer 2014, the Home Office identified a need to separate out from this risk an additional risk relating to information availability. Again, this is something that relatively few other departments have done.

The information availability risk is owned by the DRO and highlights a range of cultural and systems-related causes that may undermine the effective and appropriate management of information and records. **This is good practice.** Although the above risk description does not include non-compliance with the Public Records Act and other legal requirements among potential outcomes, it does set out a range of potential negative business outcomes and reputational impacts.

By defining and describing risks to information availability in this way, the Home Office has codified current known issues and communicated the outcome of any further issues through the department’s risk framework. Doing this underlines the impact of bad practice and positions information and records management as a current business issue rather than a purely historical issue relating to archived records.

Implementing an information risk management approach

The National Archives' Information Assurance and Cyber Engagement Programme has delivered Board-level training in addition to the IAO training mentioned above (see p. 24). Briefings on cyber-security and information risk were delivered to the SCS and Executive Management Boards in June and July 2015. According to the Home Office annual report and accounts 2014-15, a cyber strategy is also under development.

The Home Office SIRO is the Head of Corporate Services and Chief Operating Officer. The SIRO is the owner of the information exploitation risk on the corporate risk register. His sponsorship of the request to EMB members for nominations to the KIEG demonstrates that the SIRO's role of driving a supportive culture for the protection, management and exploitation of information is recognised and taken seriously. We are also pleased to note that the Home Office internal audit team has been active in this space. In addition to the 2014 thematic review of information assurance, the internal audit team looked at records management related issues for the first time in December 2014, focusing on historic file search, discovery and destruction.

One particular positive is the fact that KIM team initiatives are included as mitigating actions for the information availability risk described on the Corporate Services risk register. This formally positions planned work to improve performance in records and information management as a risk reducing activity and provides a key framework through which progress can be monitored. However, in view of the current fragmented governance for KIM discussed below (see pp. 37-8), the Home Office should ensure that it gives sufficient coverage to risk causes and mitigating actions in all areas of the business. These include OSCT, which has its own KIM team and will not be adopting iManage, HMPO and groups originating in the former UKBA where KIM governance is currently split between KIMU and UKVI KIM staff. As noted above, plans to roll out iManage in the latter areas were not yet defined at the time of the IMA while the storage of information in unstructured shared drives is likely to increase risks to its availability. **See recommendation 5**

In addition, although the risk description for information availability risk covers action needed to improve technology and guidance, the action that the Home Office needs the business to take in terms of actually following and adhering to guidance does not feature. This gap needs to be addressed, particularly as we found no evidence of information and records management related risks being documented on local risk registers. We recommend that the Home Office does so by encouraging business areas to recognise the risk of failure to comply with policy, and action to mitigate it, on local risk registers. Mitigations listed on the Corporate Services risk register should also be expanded to include action to obtain commitment from the business to comply with policy and to identify and target any areas that do not. **See recommendation 5**

3.2 Establishing control

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

Governance structures

The first meeting of the Knowledge and Information Executive Group (KIEG) took place in April 2015. The group was created with the aim of addressing a lack of crosscutting senior engagement with information management related issues, and to initiate a new system of governance for knowledge and information management. Expected functions include reviewing directorate progress, discussing risks, agreeing knowledge and information initiatives, monitoring progress, and holding the KIMU to account. Draft terms of reference issued in April 2015 position the KIEG as a senior-level ‘forum for considering and deciding knowledge and information issues’. It is clear from this document that the new body is intended to act as a proactive force that will help to involve the business in decision making and drive improvements.

The KIEG is currently expected to meet on a quarterly basis and will be chaired by the DRO and Head of KIMU; it will be attended by Senior Civil Service-level representatives from the Home Office Directorates and ALBs. These staff will assume the newly-created role of Knowledge and Information Champions, and may be represented at meetings by a deputy at a level no lower than Grade-7. The board will also be attended by subject matter experts from Home Office Technology, Corporate Security and the Office of the Chief Digital Officer. **This is good practice** and has the potential to foster effective communication and joined-up planning.

The Board's senior membership and a defined escalation route up to EMB level have the potential to provide real impetus to the Home Office's efforts to improve performance. Its creation is likely to increase central oversight and improve understanding of local dynamics. Interviewees aware of the new group were positive, with one noting: 'It is a potentially helpful means of cutting across the silos – I've heard positive things. It needs to focus on the important issues and key risks.' Another stated: 'The KIEG could make a difference as long as it gets buy in'. We strongly support the foundation of the KIEG and recommend that it receives ongoing support to ensure its potential as a force for change is reached. We understand that, following the IMA, links have been established between the KIEG and the Data Board. The DRO is now a member of the Data Board and the Head of KIM Direction is a member of the Board sub group. **This is good practice**

Supporting the business

A service level agreement is in place for Knowledge and Information Management. **This is good practice.** It covers the services to be delivered and the responsibilities of the service provider. It also establishes a relatively detailed set of expectations for how the business should act. However, while responsibilities include nomination of a member of staff at Senior Civil Service pay band 1 level to support Home Office KIM governance, the service level agreement does not mention the KIEG or the Knowledge and Information Champion role. The service level agreement is not itself mentioned in the KIEG draft terms of reference. We recommend that the service level agreement is endorsed by the KIEG. Doing this would provide a basis to hold both KIMU and the business to account. In line with our recommendations relating to information risk, we recommend that the responsibilities of business areas are extended to ensuring that staff manage, use and protect information effectively, and are not limited to simply communicating the requirement to do so. **See recommendation 5**

KIMU and KIM governance

KIMU sits in the Performance and Risk Directorate within Corporate Services. The restructured team was created in August 2014, reaching initial operating capability in March 2015. In the intervening period it has reduced from an initial size of over 100 staff towards a target size of 67 staff and has been rationalised into five teams:

- Information rights
- Information management
- KIM direction
- KIM development
- Historical inquiries and reviews

The need to reduce administrative costs as part of wider government commitments was a key driver for the restructure. The initial objective was to establish a smaller, more efficient, professional and customer-focused organisation. There was also a hope that the reorganisation would allow the new team to provide 'a single set of policies, advice, and services to all parts of a homogenous department'. Based on our review of documentation and interviews with staff, this has not yet happened.

Although individual KIM teams and KIM staff are working well and delivering benefit, the lack of a single unified governance structure can be seen in differing approaches to business planning, as noted above (see p. 19). As a consequence, it may be having a negative effect on the Home Office's ability to consistently reduce risk and drive improvements. It may be playing a part in the lack of clarity that we noted over whether responsibility for the department's unstructured shared drives lies with KIMU or IMCU. It could also be leading to risks and issues being missed in some areas of the business. For example, we understand gaps in the provision of retention scheduling for corporate information in the former UKBA were spotted following queries from the business rather than being spotted by KIMU or IMCU staff.

The lack of a single, unified governance structure for information management is likely to be a factor in a lack of clarity over where to turn for support and the limited penetration of key KIM messages in some areas of the business. During our visit to Heathrow, staff gave a number of examples of how they and their teams were working to ensure their information was better structured and managed. In most cases, local rather than central principles appeared to be being followed. KIMU itself had only limited visibility. When one interviewee, who began the interview by emphasising the importance of good records management to their group, was asked whether their team had worked with KIMU they said, ‘No – why would we?’

The creation of the KIEG offers an opportunity to significantly improve the situation, enabling business engagement and extending the reach of KIMU and IMCU. In addition, the Home Office should also establish more formal links between the DRO and head of KIMU and the IMCU and OSCT KIM teams, and a means of delivering a governance approach that cuts across group structures. This is required to support effective delivery of the new information strategy, oversight of information risk and a consistent approach to improving culture throughout the department. **See recommendation 4**

Support networks

A number of information-focused networks exist within the Home Office; of these, Records Advisers and iManagers and the information champion role within HMPO fulfil an information and records management-focused role. We were told that OSCT has its own network but that it has lapsed and needs to be re-energised. We saw evidence that the department has maintained lists of staff in the Records Adviser and iManager role, giving us a degree of confidence that both roles are currently (or have recently been) subject to central oversight. It is also clear that an active Records Adviser network has been in place, with staff mentioning newsletters and centrally-issued messages that staff were expected to communicate to their teams.

The Records Adviser’s role has been to ‘manage their unit's information on the corporate file plan and consult on, monitor and encourage compliance with best practice in information management’. Because it is focused on supporting effective use of the corporate file plan, the Records Adviser role does not cover the whole department. There are a handful of Records Advisers within Border Force, for example, but these appear to be there to support senior staff or cover key aspects such as the Border systems programme. There are no Records Advisers in Border Force to support front line staff and none at all in other areas of the Home Office, such as Immigration Enforcement.

Generally, in areas of the department where the Records Advisers should be in place, we found a mixed understanding of the responsibilities of the role. While some saw it as having responsibility for sorting out permissions, restructuring files and opening part folders, others recognised a more substantial requirement to monitor and challenge behaviours. One Records Adviser, for example, said they checked the folders they set up in the CFP to make sure that staff used them, commenting: ‘The CFP is somewhere to save business files instead of your G Drive - it’s important to use it in case someone is on leave or is absent.’

Recognition of the value that such support roles offer appeared to vary. One member of staff was keen to ensure that full benefit was obtained from the iManager role in their area as a means to drive good practice. They felt that policing should be an important part of the role and that the management chain should be used to support and enable it. By contrast, another senior member of staff gave their view that ‘Records Advisers lapse when staff leave. Their departure is not necessarily noticed and they are not necessarily replaced. Governance is needed to keep networks energised’. This is an important point because of the potential impact on the efficient set up of file structures and systems if support roles are not resourced, supported or utilised effectively.

We recommend that the KIEG is used to help ensure that the importance of networks is recognised and ensure that roles receive the support they need to drive good 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

Better policy and guidance are positioned as key enablers for the improved understanding goal in the department's Improving Knowledge and Information Management action plan. At the time of assessment, the KIM Direction team were part way through a review of policy and supporting materials due to be completed in September 2015. The KIMU action plan 2015-16 commits the team to reviewing and refreshing all policy by December 2015, and half of all supporting materials by the end of the financial year.

We are pleased to note that approval of knowledge and information policy will be part of the KIEG's role. When doing this, it should ensure that consistent branding is used and common principles are applied, while recognising individual business requirements and ways of working. **See recommendation 4**

What to Keep

The Improving Knowledge and Information Management action plan includes a clear statement that 'people in the business need to know what information to keep and how it should be managed.' A number of staff recognised the importance of this, with one saying, 'The lack of enterprise search has been a problem and the introduction of iManage should help, but there still needs to be a clearer line on what to keep.'

The Home Office has developed general guidance for staff on the retention and disposal of information and records. The guidance provides advice on whether to keep information and whether to register it as a record, and also whether it should be disposed of – this includes information that is disseminated and shared through social media and other internal and external communication tools.

Awareness among interviewees of the need to keep information with value varied. Where this was happening, staff were not necessarily drawing on corporate guidance to do so. A positive view was given by one Records Adviser, who said: ‘Guidance is fine and fit for purpose. Business information needs to be in corporate spaces – that’s easy to interpret and staff are hitting the right balance as not all emails need to be stored and staff need to sift the key things out.’ An opposing perspective came from a manager within the same group, who said: ‘I have no confidence that my teams are keeping the right things – some will be keeping too much and some too little. The challenge is significant in terms of email – capturing ebbing and flowing and evolving policy discussions. My view is that principles are not formalised and there are no hard and fast rules, with the result being redoing work and repeated discussions on the same issues.’ Across all interviewees, we found indications of varying standards in terms of information capture, titling and file structures. As one senior manager commented: ‘Records management can be patchy and is not consistent – some teams do it well, some teams not so well.’

The Home Office recognises a lack of knowledge of correct processes as a cause in the risk of important information being unavailable (see p. 33). The promotion of retention and disposal principles should form a prominent part of the work to promote information and records management requirements to all staff. This is an ideal area for the KIEG to pay attention to. It would provide a good foundation for the Home Office’s aspiration to ensure that business leaders take responsibility for the way their staff manage information. It would be enabled by the shift in focus that this report recommends, from communicating required behaviours to staff to ensuring that they are adopted. **See recommendation 5**

Providing training

The Home Office has provided different levels of training in the use of iManage as part of the rollout, with ‘embedding’ activities carried out over summer 2015 between the rollout phases. The Home Office reports that more than 100 courses have been run between the IMA and December 2015. An e-learning package has also been produced and is available to all staff.

HMPO and OSCT both provide specific training in information management and specific e-learning is available for the knowledge and information management community. There is no wider programme available to staff across the Home Office as a whole. The Home Office aims to address this and develop an electronic information management training package for use by Home Office staff. We support this idea.

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 Home Office incorporated information assurance into its existing information management maturity model – I3M – in 2013, to form a new single information maturity model, One3M. Assessing performance against the model is a mandatory requirement in six Home Office Groups and five of the department's arm's length bodies, but may be undertaken by other areas on a voluntary basis. The model was introduced with the explicit aim of helping to drive a culture of excellence in information management, embedding good information management and encouraging improved behaviours across the Group. Interviewees described One3M as 'a flexible model that changes to accommodate new areas of focus'. We saw positive evidence of a commitment to ensuring it continues to develop and evolve. This can, for example, be seen in the decision to add questions on cyber security to the 2014-15 version of the maturity model.

One3M is aligned with the HMG Information Principles, which were an output from the 2012 Government IT strategy. KIMU assesses each business area twice a year. Leads collate and present evidence and attend reviews. In the end-of-year review, likely results are discussed and a formal report is produced by KIMU. A development plan is agreed by both parties and produced by KIMU. The minimum level to be achieved is mandated each year by the SIRO. By undergoing this process annually, the Home Office expects to gradually improve its performance under each of the information principles that underpin the model. Each assessment results in a RAG rating, all of which are then consolidated into an overall annual RAG rating for the department. The score achieved by each business area is determined by the lowest score it receives under any principle.

High-level results from the Home Office's One3M information maturity model form part of the departmental security health check submitted to Cabinet Office. They are also submitted to internal audit. We were given verbal assurance that they have helped to inform future audit plans and have helped the team to focus in on specific issues. **This is good practice**

Staff in the corporate centre recognised a number of benefits derived from One3M; one stated, for example, 'You might think you know you are doing something right – this tells you whether you are.' Another commented that its use had allowed the Home Office to 're-baseline risk' after its transformation from a department of 3,500 staff to one of over 30,000.' We see this as a particularly important benefit of One3M, which has undoubtedly helped communicate the value of information across the department and the importance of managing, protecting and exploiting it effectively.

However, as the 2012 government ICT strategy that established the information principles has now been superseded, adherence to them is no longer mandatory. To ensure One3M's continued relevance is recognised, we recommend that the Home Office reviews the basis on which its model is established. It may, for example, consider rebranding the principles as Home Office rather than government principles. Doing this would put the Home Office in a good position to gain continued benefit from the use of the tool now that initial benchmarking of the department has been undertaken.

At the same time, we recommend that the Home Office addresses the following points. We found limited awareness among staff about whether their group was better or worse than others. The Home Office should consider publishing results by area to encourage an element of competition that will help raise standards. This motivation has been used successfully by a number of other departments in the IMA programme. **See recommendation 5**

We heard some criticism from interviewees about the lack of depth and insight that the model provided, with some staff surprised by how well their areas had performed in view of the shortcomings and gaps that they perceived. In our view, the focus of the questions does not reflect the Home Office's status as a single entity. For example, questions about whether policies are in place would have had more value before HMPO and the former UKBA were absorbed into the department. The existence of policies should be known now that the Home Office is a single department. We also note that the gaps in retention scheduling within the former UKBA referred to above (see p. 37) were not revealed through use of the One3M model. As staff were unaware the gap existed, they were presumably not well placed to identify it through the self-assessment process.

To support the Home Office's aim of driving business ownership of records management, the Home Office should assess whether policy requirements are being adhered to and take action accordingly. The Home Office should consider using One3M to do this. Support for this may be leveraged through the KIEG and the department's new network of senior Knowledge and Information Champions. **See recommendation 5**

Assessing progress against strategic goals

By developing and seeking support to take forward the Improving Knowledge and Information Management action plan, the Home Office has essentially benchmarked current performance and established a commitment to improve. The KIEG draft terms of reference establish the department's Executive Management Board as enablers, with an escalation route on an exceptions basis if KIEG is unable to resolve issues itself. The Home Office should also consider establishing a formal reporting requirement directly to EMB – for example, at the mid and/or end points of its new information strategy. **See recommendation 1**

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 DRO is the Head of KIM. The DRO is well-placed to exert influence on wider KIM issues, escalate risks and highlight issues and has been active in doing so. The DRO reports into the Director of Performance and Risk who, in turn, reports to the Chief Operating Officer and SIRO.

Alongside key performance-related priorities in areas including historical review and FOI performance, the KIMU 2015-16 business plan includes a commitment to achieving budget reductions in a sensible, pragmatic and fair manner. The Home Office has reorganised its FOI service to reduce the amount of work that the KIMU does on behalf the business. The historic review team reduced from a total of 20 staff to five staff, with an additional member to be recruited in January 2016. The impact of reductions in staffing numbers on arrangements for the future review of records, including appraisal and selection and sensitivity review, is unknown. At the time of assessment we were told that future transfer schedules had been mapped out through to September 2015, the point at which team headcounts were due to be finalised.

Oversight, control and use of records

The Home Office set up the Historical Inquiries and Review team within KIMU to be a coordination point for inquiries and inquests. All e-Discovery work (except for FOI) will be channelled through this team. The aim is to establish clear policies and processes. They have been involved with the Independent Inquiry into Child Sexual Abuse (IICSA) from the start and are hoping that this will help to shape their policy and process going forward. **This is good practice.**

The Home Office is engaging with The National Archives on the issue of outstanding and misplaced records, and the department is working to reduce the number of records on its outstanding list (those requisitioned for over six months). The National Archives has also recently discussed with records review staff those records that have been misplaced while on requisition.

The Home Office's corporate paper records continue to be tracked through RMSys, which was introduced in 1993 to replace manual tracking records such as ledgers and docket books. Paper customer records for UKVI, IE and BF are tracked by an alternative system (RMS) with HMPO records tracked through a third such system. RMSys was a key focus for the internal audit report commissioned at the end of 2014 in response to problems identified during the review of the department's response to historic child sex abuse allegations. The report concluded that the search functionality was unreliable and inadequate and that staff had not used the system consistently, stating that:

> *Records management has not been given due prominence in the department. As a result, staff have not been thorough in their handling and processing of historic files and an outdated system is being relied on to meet current day requirements, which are more involved than previously. Governance arrangements have been weak which means the integrity of the records management archive (database) is compromised. Current business as usual processes and practices for file recording and searching do not give us confidence that the department is providing comprehensive answers to questions asked.*

An action plan was produced following the audit. The Home Office is working to improve guidance and training for staff and is reviewing processes for bulk destruction. A project is running through 2015 to cleanse data on RMSys, imposing standard data entries where the status of records is unclear. The Home Office plans to replace the system in the future. In its 2014-15 Annual Report and Accounts, the Home Office indicated that it will 'have to accept the risk to its reputation and its ability to meet legislative obligations until this occurs'.

The 2014 permanent secretary sponsored review of paper file holdings found no significant volumes of records dating from before 1987 held in business areas. Previous office moves in 2005 are thought to have helped limit volumes of historic paper files within the business. The audit did, however, highlight the existence of some 250,000 virtual and accidentally linked case files on RMS. Staff referred to issues including failure to register case files, and duplicate files being set up. Such practices raise the risks of confusion and inaccurate decisions being taken without reference to original files. With the scale of the issue now known, the Home Office should include plans to improve the situation in the scope of its new information strategy. **See recommendation 1**

Appraisal and selection

The KIMU 2015-16 business plan includes a commitment to get historical review and transfer back on track. The Home Office accelerated review project has allowed the department to progress appraisal of paper files through to 1991. The department originally intended to select files through to the end of the 20-year transition period. A resulting delay in preparation and transfer of files to The National Archives has led the Home Office to put further appraisal work on hold while it catches up. This should improve the Records Transfer Report figures and help the Home Office to remain on track with the transition to the 20-year rule.[10] The Home Office needs to ensure that appraisal continues at the required pace. **See recommendation 6**

The Home Office has largely been carrying out appraisal by a process of file-by-file review, although it does use Series Level Appraisal Questionnaires to gather information about file series and their content. The current aim is to maintain a higher-level approach that will help the Home Office keep pace with its obligations despite having a smaller team. We support this and recommend that the Home Office further explore macro methods of appraisal. We are pleased to note that the Home Office has begun work on developing an appraisal report. This will allow the Home Office to identify, at a high level, groups of information that would be of historical value and use these to inform appraisal of both paper and digital records. **See recommendation 6**

[10] The Records Transfer Report: nationalarchives.gov.uk/about/our-role/transparency/record-transfer-report/

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

The Home Office has published its retention and disposal schedules in accordance with recommendations in Sir Alex Allan's 2014 *Records Review* report. These were last updated in 2010-11 and The National Archives was given the opportunity to contribute. We are pleased to note that the Home Office is in the process of reviewing and revising them.

As a result of the moratorium on file destruction in relation to the IICSA Inquiry, disposal of paper and digital records was on hold at the time of the IMA. To help avoid problems due to growing volumes of paper that the department cannot dispose of, the Historical Inquiries and Review team and Information Management teams have worked to identify file series of lowest risk that are unlikely to contain information of relevance to the IICSA Inquiry. The Historical Inquiries and Review team plan to carry out checks and then prepare a submission to the permanent secretary about restarting destruction of these series.

The Home Office has previously undertaken date-based disposal of records from the shared drives, excluding the CFP, which continues to use the retention schedules referenced above. The department plans to use the expected migration of digital information to iManage as an opportunity to archive material not moved across. We understand that the Home Office intends to adopt a risk-based approach to migration. This could include migrating some or all historic CFP records into the new system and treating any documents not amended for more than a year as records. The Home Office needs to ensure that a plan is in place for the disposal of records that are not moved across. **See recommendation 6**

In the frontline area we visited, staff recognised a need to separate out legacy information and were doing so by setting up separate ‘archive’ areas. This did not appear to be being done with reference to central principles. At the same time, we noted that one folder in the unstructured shared drive we had the opportunity to view included the words ‘do not delete’ in the file name. In this particular case, staff had no clarity on what the folder contained, whether the work that generated it was being taken forward or how long it needed to be kept.

The use of unstructured shared drives makes it more likely that local rather than corporate processes will be applied, which may impact on the way information is stored, structured and titled. This may increase the likelihood that business and potential historic value become harder to identify and understand, and make it harder to manage information according to its value. In addition to the risk that information with long-term value will not be protected from deliberate or inadvertent deletion, there is the risk that information that ought to be disposed of will be retained. This has potential implications in a number of areas, including the Home Office’s ability to discover information easily and its ability to comply with the Data Protection Act. The Home Office needs to improve its knowledge of the information stored outside the CFP and iManage and ensure that it has a plan in place to manage it. **See recommendation 3**

In common with a number of other government departments, some of the Home Office’s legacy databases were set up without the functionality to dispose of data. We understand that the Home Office has raised this issue with the Information Commissioner’s Office. The Home Office plans to dispose of data during future data migrations as it moves to the new common data platform. This underlines the importance of establishing a joint approach for the management of information and data in the future. **See recommendation 1**

Sensitivity review

The Home Office has had some issues with the quality of sensitivity review on files that were reviewed a number of years ago but only recently transferred to The National Archives – a small number of files were transferred open with sensitive information that had not been identified. The Home Office is working to address this by re-reviewing these files.

To date, the Home Office has largely focused on paper sensitivity review, but the department is now engaged with The National Archives' work around digital sensitivity review. Sensitivity review is carried out by the same team that does appraisal, selection and preparation of records. We were told that desk notes exist to help reviewers identify sensitivities and that, in the view of this team, the majority of sensitive information found in Home Office records is personal data. We were told that, because of this, problems can arise when dealing with complex or non-standard sensitivities.

We were told that a 10% random check is carried out of files reviewed for sensitivity, If errors are found then these are sent back to be re-reviewed. Given the recent reduction in numbers of staff, change of personnel and potential loss of knowledge, the Home Office needs to ensure that it has sufficient resource to continue carrying out sensitivity review and a clear process and guidance in place for staff to follow to ensure that as much information is released as possible and that sensitive information is protected where necessary. **See recommendation 6**

In terms of digital sensitivity review, KIMU is starting a pilot digital review exercise for a major inquiry that will centre on sensitivity review and software tools that could be used to aid the process. The Home Office needs to ensure that it continues to work alongside The National Archives in developing a process for sensitivity review of its digital information. **See recommendation 6**

Transfer and planning

Latest published Records Transfer Report figures at the time of the IMA (spring 2015) showed that the Home Office was progressing with review; however, there were still 2,278 legacy files, 2,148 files for 1987-8 and 2,278 files for 1989-90 to review. The Home Office is now (at the time of report publication) covered by a retention instrument for legacy files and files for 1987-8. The Home Office aims to clear its retained records by the end of 2016.

At the time of the IMA, the Home Office did not have a clear sense of how reduced resource and potential knowledge loss would impact on its ability to keep up with the transition to the 20-year rule. It was suggested that the Home Office might consider outsourcing this work. The Home Office needs to develop a revised forward plan for appraisal and transfer of paper files given the reduction in size of team. It should also ensure that it has sufficient resource to continue to carry out appraisal, selection and transfer of records in line with the 20-year rule transition timetable. If outsourcing is an option, then they should learn from the experience of other departments who have adopted this approach. **See recommendation 6**

The Home Office is a member of The National Archives' Digital Transfer User Group. The department is not due to transfer digital records to The National Archives until 2025. The Home Office should still ensure that it develops a plan for the appraisal, selection and transfer of digital information, learning from the experiences of other government departments and drawing on support from its Information Management Consultant. **See recommendation 6**