The National Archives

Information Management Assessment

Foreign & Commonwealth Office

Reviewed

July 2014

Published

March 2015

Working with government
to raise standards in information management

Contents

Statement of commitment

The following statement was provided by the Permanent Secretary of the Foreign & Commonwealth Office (FCO). It is published on the department's intranet site.

> In 2009, my predecessor Peter Ricketts gave his personal commitment to making sure that we create and manage the information needed to fulfil our corporate obligations to best practice standards under the Public Records Acts. I would like to reiterate this commitment, and have asked The National Archives once again to begin the process of assessment of the FCO's information management. The National Archives report will be published.
>
> Sir Simon Fraser
> Permanent Under Secretary, the Foreign & Commonwealth Office

IMA background and context

FCO first underwent an Information Management Assessment (IMA) in September/October 2009. The department subs equently produced an action plan that was signed off in 2012 following the production of a formal progress report. The action plan and 2009 IMA report can be found on The National Archives' website at: http://www.nationalarchives.gov.uk/information-management/our-services/ima-reports-action-plans.htm

FCO committed to an IMA reassessment, which was conducted in July 2014.[1] This entailed a detailed review of supporting documentation followed by interviews with senior staff, specialists and practitioners at the department's offices in London and Milton Keynes and at an overseas post. Additional telephone interviews were held in August and September of that year. This report details developments since the 2009 IMA and provides a summary of good practice and risks identified in the course of the 2014 reassessment.

[1] This was prior to publication of Sir Alex Allan's review of records management practices across Whitehall

Key findings of the assessment

1 The value of information

Key developments since the previous IMA:
• FCO has established its IT Vision 2015, which integrates IT and knowledge management outcomes • The Chief Operating Officer has been appointed as knowledge management champion

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

- FCO had no information strategy at the time of the previous IMA in 2009. The IT Vision 2015 represents a significant step forward for the department, and offers a platform for the joined-up delivery of IT and knowledge management outcomes. The 2009 IMA recommended the appointment of a board-level champion for knowledge and information management. This role was assumed by the Chief Operating Officer, who has been active both in driving the IT Vision and its Knowledge Excellence strand, and in promoting the importance of knowledge management. In addition, this report recognises that FCO currently provides its staff with a clear line through policy and guidance on the value of information and the importance of managing and exploiting it effectively.
- Phase One of Knowledge Excellence was being rolled out while the assessment team was onsite. Phase Two will centre on the replacement of the department's Electronic Records Management System (ERMS) with SharePoint 2013. Through Knowledge Excellence, FCO has the opportunity to provide a supportive technology environment that more effectively meets business needs. These include enabling oversight and control of digital records and making provision for their safekeeping, transfer and disposal in line with the department's obligations under the Public Records Act. FCO must not underestimate the significance of

this component of its IT Vision and must maintain Board-level visibility and scrutiny. This will allow the delivery of expected benefits to be monitored through to the adoption of the new system.

- FCO has used its information asset register to document key systems and IT platforms. It must now identify at a proportionate level the information assets that they contain. FCO must engage with business areas to facilitate this and achieve a more detailed understanding of the information it holds and for which it is responsible.

2 Digital information and supporting technology

Key developments since the previous IMA:
• In March 2008, FCO rolled out an interim ERMS in the form of iRecords. This is to be replaced through Phase Two of Knowledge Excellence.

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

- The current technology environment does not support the lifecycle management of digital information. FCO has put in place policy to counteract this, but the mandate is not being enforced consistently and records are distributed among the ERMS, shared drives and other locations. This raises significant challenges for FCO in terms of future appraisal and selection, safeguarding records from loss through incorrect application of disposal principles or unauthorised deletion, and in ensuring their availability for business use. FCO must ensure that staff adhere to required processes for records creation, storage and disposal now and when the new system is in place. This report recommends that FCO uses its Information Asset Owner (IAO) network to leverage information and records management outcomes and provide assurance that policy is being followed.
- Because of the limitations of the current technology environment and the level of

impact for the department if expected benefits are not realised through Knowledge Excellence, the identification and realisation of business requirements must assume considerable significance. FCO must produce a detailed plan to manage this and should engage with other departments who have or are implementing SharePoint-based solutions to ensure that known issues and risks can be identified and mitigated. As the new system is implemented, staff must be supported through necessary culture change and expectations must be managed.

- FCO should also develop a long-term strategy to realise the benefits of its new IT system, and ensure the ongoing availability, completeness and usability of digital information and records. This should target both business and information and records management-related outcomes. Plans for the migration of information and records from iRecords and the shared drives must feature within this, together with value and risk-led decisions on the decommissioning of existing systems.

3 Information risk, governance and oversight

Key developments since the previous IMA:
• FCO established its new Knowledge and Technology Directorate in January 2014. It also repositioned the Information Management Department as the Knowledge Management Department (KMD). • FCO has initiated a programme of Information Management Health Checks. Assessed areas receive a report on standards of information management and a subsequent review of progress.

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

- FCO should be commended for identifying information and records management as areas of risk in its 2013 and 2014 departmental improvement plans. However, this report strongly recommends that FCO formally defines within its risk management framework the risk of not capturing or keeping information and records in line with its value. Progress in managing this risk should be tracked as the replacement for iRecords is implemented so that changes to the department's risk exposure can be tracked. Risk descriptions within the Knowledge Management Department risk register should also be expanded to acknowledge obligations for the safekeeping of records as well as their transfer.
- As well as establishing the Knowledge and Technology Directorate, FCO has put in place a Knowledge Excellence Committee (KEC), chaired by the Senior Information Risk Owner. FCO has developed the Information Management Officer (IMO) role since the 2009 IMA, but still needs to develop a centrally-led network to drive the consistent application of standards. It is also advised that FCO defines how the IMO role can support the department's IAOs in driving compliance with corporate policy.
- FCO has made progress in defining 'What to Keep' schedules and is in the process of reviewing current policy for information and records management. Documentation reviewed by the assessment team appears consistent, but a clearer policy line is needed on the use of shared drives and the application of What to Keep schedules. Robust and enforceable processes and clear criteria must be defined in relation to weeding from the shared drives.
- The Information Management Health Check programme has helped FCO understand information and records management practice, share good practice and target areas of risk. It deserves continued support from the department.

4 Records, review and transfer

Key developments since the previous IMA:
• FCO transferred the Migrated Archives to The National Archives in 2012 and 2013. • FCO has devised a long-term, 34-year project for the appraisal,

selection and transfer of its 'special collection' files.

- Processes are being established for the review and transfer of born-digital records under the 20-year rule, starting in 2015.

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

- The Departmental Records Officer (DRO) is the Knowledge Excellence lead and is well-placed to exert influence. This report recognises that FCO has engaged at an early stage with The National Archives' Digital Transfer Project and is working to ensure oversight of paper records. It must continue to emphasise required processes to business areas and drive compliance.
- FCO is not currently meeting the transition timetable for full implementation of the 20-year rule, but is planning for transition in a more structured way than at the time of the previous IMA. FCO should work with The National Archives to agree a formal annual plan to cover the department's obligations for review and transfer of records. Plans for digital records must feature within this. FCO must also ensure continued focus on the sensitivity review of records, including ensuring that requirements relating to the protection of personal information are established and adhered to.

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 2014 IMA reassessment:
The assessment team saw evidence of a consistent message in relation to the drivers for and outcomes of effective information management within associated and supporting policy documents and guidance. The *Quick Guide for FCO information Asset Owners (IAOs)*, for example, highlights information management as an enabler in meeting obligations to ministers and the public.
The FCO IT Vision 2015 is a joint IT and KIM strategy that provides 'an opportunity to bring knowledge to the fore through IT'. It represents a joined-up approach and the Knowledge Excellence strand is explicitly aligned in support of wider strategic goals in the form of FCO's Diplomatic Excellence programme.
FCO invested effort in maintaining and improving iRecords. In particular, it enabled the automated registration of Diplomatic Telegrams (DipTels), helping to ensure the availability of these high-value records.
FCO identified information and records management as areas of risk within its 2013 and 2014 departmental improvement plans. The 2014 plan references planned mitigating actions including embedding information specialists to raise standards. The plan highlights the potential financial and reputational impact to the department of a gap in records-keeping. FCO should be commended for acknowledging this and setting out its intention to improve performance.

FCO has established a programme of Health Checks as a component of a KIM Improvement Project. These have helped identify good and bad practice and drive improvement, including via local knowledge management plans and strategies produced after Health Checks have been carried out. FCO measures performance against its own performance framework.
FCO publishes a personal data charter on GOV.UK and maintains a separate internal personal data risk policy owned by KMD. This emphasises ramifications under the department's misconduct policy and sets out escalation processes and whistleblowing procedures.
As the Head of Knowledge within the Knowledge and Technology Directorate (KTD), the DRO is on the Directorate's management team, and has a direct reporting line to the Senior Information Risk Owner (SIRO) and Chief Information Officer (CIO). The DRO is also the Knowledge Excellence Director and is recognised to have adopted an active role in steering the programme since joining the Directorate. The DRO is also a standing member of the Knowledge Excellence Committee (KEC).
FCO has clearly aligned the fulfilment of its obligations under the Public Records Act with its responsibilities under the government's transparency agenda. It is already engaging and consulting with academics in relation to its records.

Recommendations to address risk areas

Recommendation 1
FCO to provide continued corporate focus on the management, protection and exploitation of information through Phase Two of Knowledge Excellence and after its new IT system is adopted. ***This is needed to support the achievement of business outcomes and to enable compliance with the department's obligations under information legislation and policy*.**
This would be supported by: • Ensuring continuity of the information champion role. • Ensuring that progress to deliver predicted benefits under Phase Two of Knowledge Excellence is subject to Board-level scrutiny, prior to and following roll-out of the new system. • Ensuring that the risk of not capturing or keeping information in line with its value is represented at an appropriate level in the department's risk management framework. • Updating the Knowledge Management Department risk register to reflect obligations for the safekeeping of records under the Public Records Act. • Establishing an information risk policy in line with guidelines established by the Security Policy Framework.

Recommendation 2
FCO to continue to align more closely its approaches under the Freedom of Information (FOI) Act and transparency agenda.
This would be supported by: • Ensuring that transparency outcomes are explicitly factored into Knowledge Excellence. • Ensuring that the transparency team have appropriate representation on the Knowledge Excellence Committee.

Recommendation 3
FCO to build on work already conducted and liaise with business areas to identify at a proportionate level what information assets are held, their locations and their value, and log these centrally. ***FCO needs to develop a framework for the protection, management and exploitation of its information assets that focuses on broad groupings of information rather than IT systems.***
This would be supported by: • Adopting the definition of an information asset contained within The National Archives' digital continuity guidance and the Security Policy Framework and defining how this should be interpreted.[2] • Ensuring that requirements are consistently established in information management and information assurance policy and related guidance, so that Information Asset Owners (IAOs) can be clear what is expected of them. • Defining the relationship between information asset governance and records management and how the two support each other in key areas such as disposal. • Linking the identification of information assets to Knowledge Excellence.

Recommendation 4
FCO to ensure the mandate for information and records management is clearly defined and consistently enforced now and when the new IT system is introduced.
This would be supported by: • Providing a clear high-level policy line on the use of the shared drives and firmly establishing What to Keep as the basis for any weeding that takes place within them. • Engaging IAOs to provide routine assurance that corporate policy is being followed for digital records creation, storage and disposal, any weeding that takes place within the shared drives and for the transfer of paper records to Hanslope Park.

[2] See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/365742/Guidance_on_the_IAO_Role.pdf and http://www.nationalarchives.gov.uk/documents/information-management/role-of-the-iao.pdf

- Ensuring continued priority is given to the development and promotion of What to Keep schedules so staff can be clear what information has value and how it needs to be managed, now and within the new system.

Recommendation 5

FCO to establish a detailed plan for identification of business requirements and configuration of the new system.

This would be supported by:

- Identifying key lessons learned (positive and negative) from the current technology environment.
- Engaging with other government departments who use or are implementing SharePoint solutions and identifying how known issues will be addressed.
- Ensuring a close relationship between FCO and the chosen service provider is maintained to support understanding of how requirements are being met.
- Supporting the business through roll out of the new system via guidance and training, with particular focus on aspects where culture change will be required.
- Ensuring clear communication of what is changing and why, to manage expectations and establish corporate benefits.
- Considering whether the traditional distinction between 'information' and 'records' imposed by the current technology environment needs to be maintained and whether a separate records centre is the right option for records management within the new IT system.
- Ensuring that the risk of not delivering expected benefits is clearly defined and has visibility.

Recommendation 6

FCO to develop and commit to a long-term digital continuity strategy under Knowledge Excellence that centres on the principles of availability, completeness and usability.

This would be supported by:

- Embedding within the strategy plans to obtain continued benefit from the new IT system once it is in place. These may cover, for example, the maintenance of search function, metadata provision, access permissions and user groups.

- Embedding plans to migrate and de-duplicate records from key repositories such as iRecords and shared drives, and for the information and records that will be left behind.
- Embedding plans for the safekeeping and transfer of legacy and current digital records and ensuring these feed into planning for review and transfer, and assessments of time and resource required.
- Maintaining a clear vision for the provision of any additional systems or repositories under Knowledge Excellence, and clear parameters for their control.

Recommendation 7

FCO to review the current provision of IAO and support roles with a view to establishing and embedding centrally led networks.

This would be supported by:

- Formally aligning the Information Management Officer (IMO) role to Knowledge Excellence.
- Considering the appointment of designated management roles to support IAOs in the management, protection and exploitation of their information assets.
- Defining in particular how the IMO role should support IAOs in the provision of assurance on information and records management in line with corporate policy.
- Participating in The National Archives' Information Assurance & Cyber Security Engagement Programme.

Recommendation 8

FCO to continue to liaise with The National Archives as it works to ensure oversight of its records in all formats and the best use of resources.

This would be supported by:

- Liaising with The National Archives in the production of an appraisal report and formalising the link between What to Keep guidance, disposal policy, appraisal and selection under the 20-year rule and guidance for reviewers.
- Ensuring the DRO is recognised as the main conduit for discussions relating to the historical value of records and providing clear instruction on where to turn for advice.

- Working together with The National Archives to define an annual plan for review and transfer, and ensuring digital records are bought within the planning process.
- Working with The National Archives to produce a toolkit that supports the identification of sensitive personal information for use during sensitivity review.
- Working with The National Archives in the development of approaches for the sensitivity review of early digital records.

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

Over the course of the IMA, the assessment team gained a good level of assurance that FCO views information and records management as a vital area. In line with its current IT vision, FCO approaches information and records management under the general heading of 'knowledge'. The department's commitment is evident both from the appointment of the Chief Operating Officer (COO) as Board-level champion in 2012 and from the explicit emphasis attached to this area by the 2013 and 2014 departmental improvement plans. In a message to staff published ahead of the IMA, the COO emphasised knowledge management as one of the FCO Board's current top corporate priorities, stating:

> 'We create a vast amount of information every day, from political reporting and policy submissions, to our engagement with the public and businesses. Sharing this information effectively, and making sure we can retrieve what we need, when we need it is an essential part of all of our jobs.'

Information and records management policy highlights obligations placed on FCO staff by the Civil Service Code to manage information and records effectively, together with legal drivers in the form of the Public Records, Freedom of Information and Data Protection Acts. Importantly, it also highlights information's status as a corporate asset:

> 'Information management is central to the operational efficiency of the Foreign and Commonwealth Office (FCO). Information is a widely and frequently-used resource, essential to the way we work, and managing it properly is vital if we are to operate effectively and efficiently.'

The assessment team saw evidence of a consistent message in relation to the drivers for and outcomes of effective information management within associated and supporting policy documents and guidance. The *Quick Guide for FCO information Asset Owners (IAOs)*, for example, highlights information management as an enabler in meeting obligations to ministers and the public. This represents **good practice**.

Looking forward, FCO should ensure continuity of the information champion role to provide continuing leadership and leverage. **See recommendation 1**

Setting goals for information and its management

The FCO IT Vision 2015 is:

> 'To enable staff across the global network to be the best Diplomatic Service in the world, by:
>
> - ❑ providing reliable, resilient and easy to use technology across our global network
> - ❑ enabling mobile and flexible working, 'Official' where possible, classified where necessary
> - ❑ providing customer interaction and service provision which are digital by default
> - ❑ delivering information and knowledge management capabilities encouraging innovation and a culture of working together.'

The IT Vision 2015 supersedes the previous 2011–15 IT strategy. Its introduction represents a fundamental shift for the department and is one of the most significant developments since the previous IMA. The fourth 'Knowledge Excellence' strand is integrated alongside the other IT-focussed elements, providing what one senior interviewee described as 'an opportunity to bring knowledge to the fore through IT'. This joined-up approach and the explicit alignment of Knowledge Excellence in support of the wider Diplomatic Excellence programme is **best practice**.

FCO has adopted a programmatic approach to implementation with regular Board-level progress updates that have given the vision a high profile and provided regular opportunities for senior staff to interrogate progress. Joint ownership by the CIO and the Director of Communications and Engagement, helps position the IT Vision 2015 as a change programme rather than a straightforward technology programme.

Knowledge Excellence has two phases. The first focusses on increasing opportunities for connectivity and collaboration via a new intranet, networking sites and a replacement for the staff directory. Phase One was launched in Summer 2014 with a joint endorsement from the COO and the Director of Communications and Engagement. It is supported by a detailed communications plan.

Phase Two aims to introduce Microsoft SharePoint 2013 as a replacement for iRecords, the department's Electronic Records Management System (ERMS). Plans were at an early stage at the time of assessment, but through Phase Two, FCO aims to put in place an environment that will enable it to gain the most from its information. This environment must also enable the preservation and future availability of FCO's digital legacy. This report emphasises that FCO must not underestimate the complexity and significance of this component of its IT Vision. It must maintain the priority currently attached to information, knowledge and records management as Phase Two develops. It is vital that the FCO board continues to have the opportunity to oversee, interrogate and challenge progress in delivering predicted benefits as the replacement for iRecords is rolled out, and beyond this as the focus shifts to driving adoption of the new technology. **See recommendation 1**

Freedom of Information and transparency

Freedom of Information (FOI) performance is within the scope of Knowledge Excellence, which aims to introduce workflows and enable more efficient processing of requests. FCO also carried out a review of FOI performance in 2013, which raised the issue of FOI performance at Executive Committee level. This prompted the appointment of a Chief FOI Coordinator to support the Casework Team that includes a Senior Case Manager. FCO should establish a target date to return to the

Executive Committee and outline how performance has changed since 2013, highlighting any remaining obstacles. **See recommendation 2**

Published statistics indicate relatively consistent performance in meeting obligations under the FOI Act. FCO conducts a high number of public interest tests, which is reflected in the low volume of requests that meet the initial 20-day deadline. However, with the exception of the period October–December 2013, FCO has been above the threshold of 85% of requests answered 'in time' that can trigger a period of monitoring by the ICO. The latest available statistics at the time this report was drafted show that FCO answered 93% of requests in time between April and June 2014, which is in line with the average across all monitored bodies and above average among departments of state for this quarter. The 2013 annual review of FOI performance shows that FCO undertook 69 internal reviews during the year, of which 72% were upheld in full – slightly below the average for departments of state at 75%. Nine appeals were made to the Information Commissioner's Office during the period. Of the four whose outcome was known at the time of end-of-year monitoring, all were upheld in full.[3]

At the time this report was drafted, FCO had published 2,600 documents on GOV.UK, including transparency data and policy documents. FCO should also be commended for the January 2014 hack day, which aimed to highlight and utilise data already published by the department. There is, however, limited mention of transparency outcomes within Knowledge Excellence documentation. FCO would benefit by continuing to enable closer formal collaboration between the FOI team, which sits in the Knowledge and Technology Directorate, and the transparency team, which sits in the Communication Directorate. This report recommends that FCO builds open data and transparency outcomes into its IT Vision 2015 and ensures appropriate representation on the standing membership of the Knowledge and Excellence Committee (KEC). **See recommendation 2**

[3] https://www.gov.uk/government/collections/government-foi-statistics

1.2 Managing information as a valued asset

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

Ownership of information assets

Information Asset Owners (IAOs) within FCO are appointed at Director and Head of Post level. This gives the role a significant degree of authority, but means that IAO duties are delegated on a day-to-day basis. FCO asks its IAOs to provide assurance on their information assets once a year as a component of the Annual Consolidated Certificate of Assurance (ACCA). This is in line with the minimum requirement established in Cabinet Office guidance on the IAO role.[4]

Defining and cataloguing information assets

FCO launched a project to compile an Information Asset Register (IAR) in 2011. This focussed on capturing context about accredited IT systems in the UK and overseas, with the subsidiary aim of identifying any further systems that were not catalogued once the IAR was established. Further work was undertaken in 2013, adapting and developing the IAR template to collate a wider range of context. Because of this, the IAR was expanded to include additional columns relating to digital continuity, wider risk and suitability for release under the government's transparency agenda.

The current FCO IAR represents a positive start, but FCO must now build on it and achieve a more detailed level of oversight. It has not yet identified the broad groupings of information that are held within its systems, platforms and hardware. These are created and owned by business units and should be the focus of an organisation's framework for managing its information assets. Because the FCO framework does not achieve this level of detail, its usefulness as a management tool is limited. For example, iRecords is listed on the IAR together with the Confidential and Universal tiers of Firecrest, which host the department's shared drives. These

[4] Cabinet Office guidance for IAOs sets out actions needed to meet the requirements of the Security Policy Framework: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/255914/Guidance_on_the_IAO_Role.pdf

locations should contain the majority of the department's most valuable information. However, because the information assets within these systems have not been defined, FCO is unable to identify through its IAR what open data or transparency-related material is held within them.

The assessment team also notes that the department's high-level approach may have an impact on the assurance received from its IAOs. The Security Policy Framework requires IAOs to 'understand what information is held, what is added and what is removed, how information is moved, and who has access and why'. IAOs need to be clear what information they are accountable for, and how the information generated and owned by their directorate or post should be broken down and understood. From an assurance point of view, it is crucial that the information assets created and owned by departments and posts and held within corporate systems are clearly identified. At the same time, IAOs need the right training and support.

As a first step, this report recommends that FCO formally adopts the definition of an Information Asset within the Security Policy Framework and The National Archives' digital continuity guidance. It should ensure that a single definition is used and that this is conveyed and interpreted consistently in supporting policy and guidance. FCO should then engage with business areas based on this definition to identify, at a proportionate level, the key information assets that are held and their locations. This may, for example, be achieved by focussing on individual IAO's directorates or posts and should be information and value led. Doing this would provide a firm foundation from which to move to the department's new IT system and help to identify what information needs to be migrated across. **See recommendation 3**

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

FCO provides three shared repositories that can be used to store digital information. These are:

- The ERMS, iRecords, which is nominated as the main corporate repository for digital records.
- SharePoint 2007 TeamSites, which are not subject to central governance and are reportedly still officially classified as a pilot.
- Shared drives, which act as the default working area and repository for team information with a short-term business value of up to two years.

The current technology environment supports the lifecycle management of digital information and records to a limited degree only. There were some positive views from individuals that iRecords acts as a 'filter for important documents' and for 'anything relating to departmental chronology'. However, iRecords was introduced as an interim storage solution and allows creation and secure storage, but does not support disposal – a core required characteristic of records systems identified in the section 46 Code of Practice.[5]

The shared drives offer a potential means of reducing the impact of this by providing a shared repository for information without long-term business or historic value where disposal is possible. Such information is defined in the department's shared drive policy as having a business value of up to two years. FCO has also sought to encourage storage of information with longer term value in iRecords by allowing the

[5] http://www.justice.gov.uk/downloads/information-access-rights/foi/foi-section-46-code-of-practice.pdf

establishment of ‘quick links’ in shared areas that allow low-barrier, two-click registry within the ERMS. However, these factors must be balanced against the fact that shared drives offer limited protection from the accidental or unauthorised alteration, copying, movement or deletion of records not transferred to iRecords. If records with long-term business or historical value are stored within shared drives, then they can be deleted.

FCO has worked to achieve a 21% increase in registration of records in iRecords during the financial year 2013–14, and the department should be commended for this. However, records are undoubtedly held in other locations and the assessment team saw limited evidence that information is yet being saved consistently to the ERMS in line with its value. Shared drives remain the repository of choice for some staff interviewed. One member of staff, for example, stated that information in their team’s shared drives dated back to at least 2006. At an extreme, some staff interviewed at post stated that they knew iRecords existed but had never used it, or that they were encouraged to use the system but did not. One interviewee stated that staff do not use iRecords because they either do not know about it or do not see any benefit in using it, commenting, ‘staff are busy and iRecords is slow.’ Another said, ‘it’s a slow process and frustrating. iRecords is *not* user friendly. You twiddle your thumbs while various boxes pop up’.

If the expected benefits of the FCO IT Vision 2015 are realised, then key barriers to records creation will be reduced. However, this by itself is unlikely to be sufficient to embed effective records management in practice, and FCO will need to ensure principles are followed and systems are used appropriately. This is particularly important because responses from staff at all levels strongly indicated that the mandate for information and records management is not currently being enforced consistently, with adherence to policy varying across the department. This could be seen in descriptions of practices by individuals and teams, in references to differing practices found on joining new business areas and in explicit comments made by interviewees. One stated, ‘there are no penalties, and there is an expectation that you will hit the ground running – people can move on and not care’, while others asked ‘if this is so important then why is it not enforced?’ and a third questioned the

penalty for non-compliance compared to a lapse in information security, asking ‘what is the punishment?’

In addition to developing its information asset framework, this report recommends that FCO does more to engage its IAOs now and in the future as a key avenue to drive good practice in records creation and disposal. FCO must also identify how the policy mandate will be enforced within the new IT system. **See recommendations 3 and 4**

Ensuring the availability of information

A reliance on personal repositories can raise a number of challenges to digital continuity. In particular, valuable information may not be complete because key context is missing or may not be available according to business need. This report recognises that FCO has made efforts in this area by encouraging use of shared areas and limiting the size of personal drives, which appeared to be relied on less by staff than at the time of the 2009 IMA.

This report also recognises that FCO has also promoted the use of instant messenger for ephemeral conversations and tried, through guidance, to encourage staff to adopt alternatives to email where appropriate. Email remains an area of vulnerability for FCO, however. The risk that information stored outside shared areas may be lost to the organisation is made more likely to manifest by the fact that staff tend to move once every three years, and the assessment team heard conflicting accounts of personal drives and email accounts being deleted when this happened. A number of staff stated that they used personal email accounts to get around this, which is problematic as personal accounts are very likely to be less secure than FCO’s corporate email accounts. In addition, although email limits are in place, these have been recently relaxed for business purposes, which may remove an incentive to transfer emails to shared areas. Finally, interviewees mentioned using .pst files. These allow the storage of large volumes of information in a compressed format, which magnifies the risks associated with personal storage, including making it easier to export very large volumes of data outside the organisation. Emails stored in this format may also be less stable and more subject to corruption.

The automated registry of Diplomatic Telegrams (DipTels) within iRecords was highlighted by a number of interviewees as a key means of ensuring the preservation and therefore the long-term availability of a high-value resource. FCO should be commended for putting this policy in place. Interviewees saw benefit in iRecords as a repository of historic records, with one noting that it should be easier to find information stored within it because its value had already been identified. Although FCO is now no longer investing in improving the system in light of the forthcoming move to Microsoft SharePoint 2013, some staff also stated that its usability had increased over time. However, others took the view that confidence in the findability of information in iRecords remained low, due to a poorly developed search function.

iRecords links can be emailed, which supports the provision of a single authoritative version. However, across the technology environment as a whole, a number of interviewees said they encountered difficulties relating to version control and finding information in line with business need. This included evidence of decisions taken and protocols and procedures previously followed. Reasons given by interviewees for difficulties finding information that they felt was held by FCO included varying file structures and architecture, inconsistent naming of files and the number of results obtained from searches. One member of staff commented that you can only find information if you know where to look, and others mentioned duplication and overlap.

In the short term, FCO must maintain a focus on how information should be stored and structured to support findability and exploitation. In the longer term, FCO must ensure lessons are learned in relation to ease of use of systems, the availability of information and version control, and factor these into Knowledge Excellence. These include elements that work well as well as those that do not within the current technology environment. **See recommendations 4 and 5**

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.

The move to SharePoint

The geographic distribution of FCO, coupled with the requirement to handle sensitive information, raises significant challenges for the department's IT infrastructure. Through the Knowledge Excellence strand of the IT Vision 2015, FCO has a unique opportunity to address many of the issues highlighted in this report and provide a truly supportive technology environment. To achieve this, FCO must ensure that business requirements for information and records management are at the core of the project. If requirements are not identified correctly then there is a risk that the new system will not meet business needs or deliver expected benefits in preserving the department's digital record.

FCO should develop a detailed plan to cover the identification of business requirements and the configuration of the new system to enable their achievement. This should be directed towards the digital continuity outcomes of completeness, availability and usability.

Clear communications will be needed to manage change. FCO should ensure it has a good understanding of known issues in relation to SharePoint and records management and their implications, including metadata management, records export and team site deletion. Third-party solutions in particular may be needed to enable MS Outlook integration, which is not supported by SharePoint 2013, and for records disposal. Requirements in this regard were not yet fully determined at the time of assessment. These should be prioritised. This report recommends that FCO uses senior KIM networks and draws on the growing body of knowledge about SharePoint within government. It should engage with departments in the IMA programme such as the Department of Health and the Department of Energy and Climate Change which have or are adopting the system. **See recommendation 5**

FCO's early plans for the new IT system focus on the establishment of a separate records centre. This approach relocates records to the records centre, leaving a 'stub' in place to facilitate continued access. However, this is one of a number of possible options for records management, including management in place and collaborative working within the records centre. FCO needs to choose the right

option from a cultural and a records management point of view. In terms of the latter, it is important to recognise the emphasis that the records centre approach places on content types, rather than the function that created the record and the teamsite in which it originated. In terms of the former, FCO should consider whether it needs to maintain the distinction between information and records imposed by the current technology environment. In practice, all information generated by the department is a public record. Separating out information with potential historical value may impose an artificial barrier in the mind of staff meaning that they do not see 'the records' as something with current business value to them and their colleagues. By extension, it may lead them to overlook requirements for the management of other information that is not designated as 'a record' by its location. **See recommendation 5**

Digital continuity planning

Once the new IT system is in place, FCO needs to ensure full value can be obtained from it. This is likely to involve considerable effort in terms of governance behind the scenes. It will be crucial, for example, to drive the correct set-up and use of team sites and in the management of Active Directory groups. Ongoing focus on search capability will be crucial to success, with an emphasis on ensuring the creation of good metadata to enable good-quality search results. This should include looking at standardised thesauri and classifiers. It will also be crucial to ensure that information with historical value remains usable until it is due for transfer. To facilitate this, FCO should establish a digital continuity strategy aligned to Knowledge Excellence.

FCO's digital record is not exclusively in iRecords, but distributed across a number of systems including the shared drives. The department needs to ensure the ongoing availability and completeness of records held in all locations, not just iRecords. At the time of assessment, no decisions had been made about the volume of records that will need to be migrated to the new system, how records will be de-duplicated, and how any records not moved will be managed. These considerations should form a central element of FCO's strategy. FCO should also factor in plans for the decommissioning of systems and repositories such as the old intranet. In particular, FCO should ensure a clear plan is established for the shared drives. **See recommendation 6**

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

Defining information risk

Knowledge Excellence and FCO's IT Vision 2015 are both explicitly risk driven. Together, they are intended to address current threats to and increase opportunities for the effective management and exploitation of information. This report also notes that FCO identified information and records management as areas of risk within its 2013 and 2014 departmental improvement plans. The 2014 plan includes mitigating actions such as embedding information specialists to raise standards. It also highlights the potential financial and reputational impact to the department of a gap in records keeping. FCO should be commended for acknowledging these impacts and setting out its intention to improve performance.

The Knowledge Management Department (KMD) maintains a risk register that is owned by the head of department who is also the Departmental Records Officer (DRO). The register features four risks relating to the timescale for delivery of Knowledge Excellence, compliance with FOI and Data Protection Acts and ability to meet obligations for transfer under the Public Records Act. This report recommends that the department's obligations for safekeeping of records, which, in digital terms, extend to ensuring their ongoing usability, should also be referenced. **See recommendation 1**

The assessment team were unable to confirm what information and records management-related risks, if any, are formally recognised above the level of the KMD register. To aid clear communication and effective decision making, this report recommends that FCO should formally define the risk of not capturing and keeping information in line with its business or historical value. A number of factors make this

particularly important: the likely current distribution of the FCO's record outside iRecords, the replacement of the ERMS, the need to migrate information to the new system and the need to ensure continued access to records. In defining this risk, FCO must ensure that a full range of mitigating factors is recognised including, but not restricted to, the Knowledge Excellence programme. This risk should be monitored as the new IT system is rolled out and adopted. **See Recommendation 1**

Implementing an information risk management approach

FCO publishes a personal data charter on GOV.UK and maintains a separate internal personal data risk policy, owned by KMD. This emphasises consequences of breaches under the department's misconduct policy and sets out escalation processes and whistleblowing procedures. This is **good practice**.

The FCO information security policy has been updated a number of times since it was created in 2007. The last changes were approved in February 2012 and the document has no schedule for future review. A separate March 2014 FCO information risk policy establishes expectations under the Service Management Integrator (SMI), focussing on systems and technical capabilities. It sets out requirements for system accreditation while emphasising that FCO remains accountable for the risks to the department's information.

Neither of these two policies meets requirements established under the April 2014 Security Policy Framework for a Board-owned information risk policy. FCO should ensure that such a policy is developed and put in place. It should use it as a means to establish clear principles in relation to information and records management-related risk, and set out the department's strategy for addressing them. **See recommendation 1**

3.2 Establishing control

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

Supporting the business

The Knowledge and Technology Directorate (KTD) was established in January 2014, replacing the previous Information and Technology Directorate. The restructure was positioned as a means of bringing about a 'transformational change' in the way IT, tools and services are provided to FCO and of initiating a more collaborative relationship with the business. KTD is led by the Senior Information Risk Owner (SIRO) and Chief Information Officer who is also the Knowledge Excellence Committee (KEC) chair. At the time of assessment, the directorate consisted of Strategy and Engagement and Technology divisions together with KMD, where the KIM team is sited.

The assessment team gained a good level of assurance that this governance structure is one that can support close collaboration between knowledge and IT professionals, and planning towards shared information goals. This is a crucial first step in assuring the department's digital record, and FCO must continue to sustain the priority that is currently attached to KIM objectives. **See recommendation 1**

At the time of assessment, the KIM team was heavily involved in the delivery and promotion of Phase One of Knowledge Excellence. A high priority was attached to this work, both for its own purposes and as a 'shop window' for Phase Two. KMD is also delivering a large part of the online resources for the new Diplomatic Academy.

The assessment team saw evidence that the KIM team is working proactively to improve standards of information and records management within the business. The KIM team has five members whose focus is on delivering policy and engaging with the business to understand and improve performance. This report particularly highlights the setting of targets to increase registry within iRecords and the team's programme of Health Checks as a component of a KIM Improvement Project. Although some senior staff interviewed questioned the visibility of the Health Check programme, the assessment team saw evidence of local knowledge management plans and strategies that had been produced following assessment. Health Checks have delivered benefits by targeting key areas of the organisation such as Private Office and using assessments as an opportunity to challenge behaviours. They have

also promoted key elements of good practice, including the incorporation of information and records management within inductions and the use of Handover and Knowledge Cards. The assessment team was given assurance that individual assessments will highlight the need for stronger lead on information and records management if required. It is clear that FCO is currently working actively and using a number of different approaches to encourage good practice and adherence to corporate policy.

Support networks

The work of the central KIM team is supported by a number of part-time information-related roles held by FCO staff. These include Information Management Officers (IMOs) together with Open Government Liaison Officers (OGLOs) and IT Support Officers. IMOs in particular have a key role to play in ensuring the appropriate and effective management of information and records in shared drives and iRecords.

The 2009 IMA report noted that FCO could be using the IMOs more actively as a resource beyond iRecords administration. IMOs interviewed appeared committed to their roles and it was apparent that a number had volunteered, rather than being nominated by their managers, because they recognised the benefit to the organisation of good practice in information and records management. A number of IMOs interviewed were engaged in work to improve standards including through the improvement and development of filing structures. There was also indication from some interviewees that the IMO role was reflected in performance objectives. However, although the assessment team saw some evidence of local informal liaison between IMOs, the IMO network as a whole did not appear to be particularly active. In some areas, the role was not resourced or had been left empty after the departure of the role holder.

FCO should review the current allocation of support roles and should consider rebranding and re-energising the IMO role to bring it into line with Knowledge Excellence. This report also recommends that FCO establishes a formal IMO network. Leadership from KMD and support from FCO is needed to ensure that the role is resourced, is given sufficient priority and a platform to influence, and has

continuity when staff change or leave jobs. FCO should also define formally how the IMO role supports IAOs in the provision of assurance on the management of their information assets. **See recommendation 7**

3.3 Providing direction

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

Knowledge and Information management policy and guidance

Information and records management policy and guidance were under review at the time of the 2014 IMA reassessment. An updated version of the Information and Records Management Policy was published in June 2014. The policy was first created in 2005, and has been reviewed periodically since then. The June 2014 update follows a minor update in 2011. The new version of the policy reflects the current KTD structure and is signed off by the CIO and SIRO. This is **good practice**.

The information and records management policy is currently accompanied by a set of supporting policies covering shared drives and iRecords and key topics such as records destruction, email management and vital records. Policies are relatively consistent with each other and contain many good practice elements, including a clear statement that establishes records as the collective memory of business units and FCO as a whole:

> ‘Records constitute the collective memory of the business unit or post and ultimately of the FCO. They are needed now and in the future to provide an audit trail for the development of any given policy, or the background to a decision. The documents created and stored today in the FCO are the public records of tomorrow.’

However, a few gaps and inconsistencies are evident. In particular, the main information and records management policy establishes a narrative in relation to the problems of shared drives usage, but does not provide a clear, high-level statement on how they should be used, or link to or reference the supporting shared drive policy. This must be addressed. **See recommendation 4**

The *Quick Guide for IAOs* lists a 'regular programme of weeding to ensure you are not retaining redundant or obsolete files' under key areas of assurance covered by the Annual Consolidated Certificate of Assurance (ACCA). The need for regular weeding is also referenced in the shared drive policy. However, while this lists What to Keep guidance under a list of related polices, it provides little context on how weeding should be conducted or by whom. The *Quick Guide for IAOs* and the shared drive policy are not cross-referenced, and the former does not mention What to Keep. It is also not mentioned within information and records management policy, although this does specify that guidelines for disposal need to be agreed with the Knowledge Management Department. The assessment team notes that the agreement of such criteria was not covered in sample Information Health Checks supplied for review.

In view of the likelihood that records with historic and long-term business value will be held in the department's shared drives, robust and enforceable processes must be in place to control any weeding that takes place. What to Keep schedules must be the basis for this. IAOs should be explicitly engaged to ensure that this is understood, and provide assurance to the DRO and SIRO that guidelines have been agreed and are being followed. **See recommendation 3 and 4**

KMD has produced generic What to Keep guidance and offers support in the generation of tailored schedules through the Information Management Health Check programme. FCO should continue to prioritise the use and application of What to Keep, which will have ongoing value in providing a basis for disposal processes within SharePoint 2013 and migration planning. From a cultural point of view, and in light of the regular rotation of staff between roles, What to Keep also offers benefit in

providing a statement on what information a particular team produces and works with and what its value is. **See recommendation 4**

3.4 Measuring impact

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

Measuring compliance with policy

Health Checks have been highlighted in the 2013 Cabinet Office *Security Risk Management Owner Good Practice Guide* and have been subject to scrutiny by FCO's internal audit function. These are being conducted according to a defined plan and cover overseas posts as well as UK-based directorates.

The programme delivers reports and recommendations, targeted to directors and heads of post, and assesses progress after twelve months. Assessed areas are measured against an FCO maturity model based on the Knowledge Council model. Reports are detailed and tailored; FCO should continue to support this programme and ensure that action can be taken where a lack of engagement is found. As well as delivering individual recommendations, to maximise the benefit for FCO, the Health Check team should consider delivering a summary of good practice and common concerns to the KEC.

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

As the Head of Knowledge within KTD, the DRO is on the Directorate's management team, and has a direct reporting line to the SIRO and CIO. The current DRO is also the Knowledge Excellence Director and is recognised to have adopted an active role in steering the programme since joining the Directorate. The DRO is also a standing member of the KEC. This is a **good practice** arrangement that has the potential to give the right level of priority to information and records management objectives and to support clear and direct communication of related risks.

FCO should ensure that the DRO maintains this profile. FCO should also ensure that the DRO is recognised as the main conduit for contact with The National Archives and discussions relating to possible selection of records from all directorates and posts. **See recommendation 8**

Oversight of records

FCO paper records can be split into two groups: records due to be transferred to The National Archives under the 20-year rule and the 'special collection' files. The latter were placed under a Lord Chancellor's Instrument until December 2014 to allow FCO to devise a plan for their appraisal, selection and transfer alongside business-as-usual records. A long-term, 34-year project is now in place.

FCO aligns its obligations under the Public Records Act with its responsibilities under the transparency agenda, and is seeking to engage and consult academics in relation to its records. This is **good practice**, and The National Archives recognises the department's firm commitment to transparent process. The department publishes an inventory giving estimates for the number of standard departmental files held at

its repository at Hanslope Park and within the special collections. This is described by FCO as a continuously evolving document that will be regularly updated.

FCO has clear procedures in place requiring the regular transfer of paper files held in departments or posts. The assessment team received a good level of assurance that FCO is seeking to ensure it has oversight of these records by keeping an inventory of records and unregistered holdings. In March 2014, for example, the Chief Operating Officer wrote out to all Directors reminding them of their obligations under departmental policy and asking for assurance that transfers from posts and unnecessary paper files are not being retained. FCO should be commended for this high-level intervention. In September and October 2014 following the IMA reassessment, FCO carried out a file audit at record series level which encompassed paper files held across the UK estate. In addition, the assessment team understands that overseas missions were asked to declare their paper file holdings at record series level. FCO provided the resulting inventory to the Advisory Council, for consideration at the Council's meeting on 13 November 2014.[6] The department requested administrative retention for one year to provide time to develop a prioritised plan for the review of the material identified during this audit.

FCO needs to maintain a focus on driving compliance with requirements for safekeeping and selection of records under the Public Records Act. FCO must ensure that posts understand their responsibility in this regard and know where to turn for advice. A number of interviewees asked the assessment team questions about records held locally that they perceived to have value, but were unsure what to do with them. **See recommendations 4 and 8**

FCO holds early Automation and Electronic Registry System (ARAMIS) digital records in the form of simple text files that have been incorporated into the department's legacy Minerva system. This holds approximately four million records. FCO moved those below Secret level to iRecords in 2013 to improve their accessibility ahead of appraisal and selection. ARAMIS records cover the period

[6] Context on the Advisory Council's role can be found here: http://www.nationalarchives.gov.uk/advisorycouncil%5Cdefault.htm

1992–2000 and will be due for transfer in 2017. FCO is likely to be one of the earliest departments to transfer digital records to The National Archives. This report recognises that FCO has actively engaged with The National Archives on these records at an early stage and that FCO is a pilot for the Digital Transfer Project. It must now ensure that this is brought within wider planning, to ensure an accurate assessment of time and resource required can be made. **See recommendation 8**

While FCO staff expressed a good level of confidence about the robustness of the ARAMIS record, there was a common view that the digital record that comes after it will be more problematic. Backlogs in registering files and inconsistent use of iRecords mean that the digital record is likely to be distributed across shared and personal information stores. This problem is made more significant by the inconsistent management of the shared drives.

The assessment team understands that FCO began work on an appraisal report following the 2014 IMA reassessment. This offers a means of ensuring the department has a clear statement on what records are selected for the public record in the future. FCO should engage with The National Archives in this work and ensure that it consults with a range of stakeholders as the report is developed. The National Archives views the production of an appraisal report as an important step in guarding against future digital backlogs. It will have added benefit in ensuring that directorates and posts understand the value of records they hold that are worthy of selection and eventual transfer to The National Archives. FCO should then ensure that it is able to maintain its understanding of what information it holds. In particular, it should formalise the link between What to Keep guidance, disposal policy and appraisal and selection of records under the 20-year rule. **See recommendation 8**

4.2 Implementing disposal decisions

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

Sensitivity review and planning to transfer

In common with the Cabinet Office and the Ministry of Defence, FCO holds a considerable volume of sensitive material up to a top-secret level. These records include diplomatically sensitive material with a possible impact on the UK's international relations and material relating to the security and intelligence agencies.

In September 2014, FCO outsourced paper file listing, cataloguing and physical preparation. The department's sensitivity reviewers undertake selection and sensitivity review on a file-by-file basis. In view of the scale of this challenge, FCO is recruiting further reviewers to complement the team of 29 part-time staff that are already in place.

Sensitivity reviewers are former members of staff. Those interviewed indicated that they worked on records related to areas of the world that they had previous experience with. The team of reviewers is divided between London and Hanslope Park. At the time of assessment, re-review of closed records and re-examination of exemptions in those closed records was identified as a key priority alongside business-as-usual work.

Justifications for the closure or retention of FCO files are completed by individual sensitivity reviewers, who may refer files to other departments or agencies when they judge that a view on potential sensitivity should be sought. Decisions are quality-checked by the lead reviewer. The National Archives recognises that the reviewers represent a huge asset to the department and that their knowledge and experience is invaluable. A consistent system is now in place for selection and sensitivity review and a checklist has been developed to formalise the review process and assist sensitivity reviewers in decisions on closure or redaction. However, while FCO is well-placed to identify diplomatic sensitivity, there remains an ongoing need to emphasise requirements in relation to personal information. FCO also faces a challenge in terms of digital sensitivity review where there is duplication between early digital records and paper records. FCO is consulting with The National Archives in both areas as it works to ensure the consistent application of principles.

See recommendation 8

Transfer and planning

FCO has transferred 23,163 pieces to The National Archives between the 2009 IMA and 2014 IMA reassessment. In addition, following the Cary Report commissioned by the Foreign Secretary in 2011, the Migrated Archives was transferred over the period 2012–13.[7] This consisted of just under 20,000 files. FCO worked closely with The National Archives throughout this process, with FCO records staff attending bespoke training sessions at Hanslope Park.

FCO is not currently meeting the transition timetable and on current plans will not meet the 2023 deadline for full implementation of the 20-year rule. This report recognises, however, that the department is committed to getting back on track and has invested considerable time and resource in doing so. FCO has clearly sought to learn lessons from the Migrated Archives, and has recognised the importance of accurate records inventory figures to support public communication, planning and resource allocation. In particular, FCO is applying a project methodology, with documented work practices, both to the special collections and to unregistered material that sits outside the yearly file review process. FCO has proactively engaged with the Advisory Council and applied for Lord Chancellor's Instruments (LCIs) for the retention of the special collections and its annual transfers. **This is good practice.**

This report recognises that FCO is planning in a more structured way than at the time of the 2009 IMA. In view of the complexity and value of the records involved, this report recommends the production of an annual documented plan for review and transfer that is agreed with The National Archives. **See recommendation 8**

[7] The Cary Report can be accessed here: https://www.gov.uk/government/publications/cary-report-on-release-of-the-colonial-administration-files