The National Archives

Information Management Assessment

Cabinet Office

Assessed: August 2013

Published: July 2014

Contents

Statement of commitment by the Cabinet Office

The Cabinet Office holds some of government's most important records, and as a department we are committed to making sure that we manage and protect them. An important part of our duty under the Civil Service Code is to keep accurate official records and handle information as openly as possible within the legal framework.

The National Archives regularly conducts assessments of Information Management practices and compliance within government departments, and to show the strength of our commitment to best practice I have asked them to review Cabinet Office processes and systems.

The following report will help me to support records management processes across the department, so that the right information can be appropriately captured, managed and preserved for the nation.

Richard Heaton, Permanent Secretary, Cabinet Office

Overview and IMA scope

The Cabinet Office is a predominately outward-facing Department with wide-ranging pan-government responsibilities. Its focus is on delivery through other departments with civil service wide responsibilities. It holds extremely valuable information that is a legacy to the nation.

The Information Management Assessment (IMA) of the department's information management and information assurance activities enables The National Archives to assess to what extent Cabinet Office's governance is sufficient to monitor and enforce internal standards to the same level as its external responsibilities.

IMA background

The Information Management Assessment (IMA) entailed a detailed review of supporting documentation followed by interviews with senior staff, information and technology specialists and others. These were conducted in the period 24 June–8 August 2013. Further evidence was sought after the review, this and the department's need to focus on new IT plans and FOI performance issues alongside other competing priorities in both the Cabinet Office and TNA has meant that it has taken longer than usual to finalise the report.

The following report provides a summary of good practice and risks identified in the course of the assessment. IMA reports and departmental action plans are published on the National Archives website and can be accessed at:

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

Executive summary

Cabinet Office is at the heart of government, with responsibility for national security, foreign affairs and the civil service. It sets the strategic direction of government and has wide-ranging pan-government responsibilities that include information assurance (IA). To deliver its remit internally it needs to ensure that its internal governance standards are as robust and on a par with the standards it establishes externally.

The value of information

Communicating and realising value	**Satisfactory**
Managing information as an asset	**Development Area**

- Cabinet Office is constantly evolving as new external policies are developed and taken forward. This presents a particular challenge for knowledge and information management within the department. The assessment team noted pockets of excellence within Cabinet Office, where information was managed effectively and its value was understood, but this was not consistent across the department.
- Cabinet Office's Information Strategy is aligned to the Information Principles for the UK Public Sector and embraces a set of key information related policies and strategies, including knowledge management. However, penetration of the Information Strategy and its supporting documents is not consistent across the department. Without consistent direction, information may not be managed according to value and adherence to internal policies may be dictated by local business priorities. This has a direct bearing on Cabinet Office's ability to safeguard its legacy information across the whole of its remit.
- Strong governance is key to ensuring the priority of information goals is recognised and to supporting effective policy and strategy implementation. There was confusion around specific information management and information assurance responsibilities of the Senior Information Risk

Owner (SIRO), Chief Information Officer (CIO), Departmental Records Officer (DRO) and Information Asset Owners (IAOs) and how these roles and responsibilities interlinked and contributed to Cabinet Office's compliance activities. Each was clear on their responsibilities but there is less cohesiveness where there is cross over. When the review was conducted, corporate governance had recently changed in the department. The former governance body (the Information Strategy Board) had been disbanded and its responsibilities handed up to the Executive Management Committee (EMC) under the direct oversight of the Permanent Secretary. There is, however, no longer a forum for stakeholders to discuss internal information management policy, issues and impacts in more detail. Based on experience of best practice examples in government, The National Archives recommends that Cabinet Office bolsters its governance structures by convening an internally focussed discussion group to support the governance provided by EMC.

- The Cabinet Office's 2010 What to Keep strategy, Managing Information, and individual signed 'What to Keep' agreements are drafted on best-practice lines. However, agreements are not in place for new policy areas. Addressing this will help ensure key decisions are kept across the whole department and its legacy is preserved. Cabinet Office has the opportunity to be innovative in integrating this work with other departmental initiatives such as raising Freedom of Information (FOI) performance.
- Cabinet Office's overarching approach for information asset Management was not clear and understanding of information assets was conceded to be 'patchy' by several senior level interviewees. The appointment of Heads of Business (HoBs) as IAOs had a positive impact as the roles gave a sense of importance, responsibility and priority. Training for the role should be promoted.

Digital information and supporting technology

Supporting information through technology	**Development Area**
Supporting digital information through change	**Satisfactory**

- Within Number 10 Downing Street, the assessment team saw evidence of effective management of electronic correspondence through the 10 Share system. In the wider department, Cabinet Office’s digital information is captured across a variety of non-interoperable systems, including two Electronic Document and Records Management Systems (EDRMS): Meridio and Retriever; and the FLEX system for highly classified information. Shared drives are also in use. These are managed by the external IT contractor. The assessment team found that most staff use Shared drives in preference to the EDRMS because they are perceived to offer quicker and easier access to information.
- Growing volumes of digital information are stored across these systems. Digital systems do not have switched on, automated retention schedules and there is no consistent plan for the disposal of the information they hold. Cabinet Office needs to address this issue now, by ensuring that relevant risks are defined and highlighted, and by putting in place appropriate mitigating actions. Cabinet Office has the opportunity to address the need for actionable retention schedules, together with other risk areas identified in this report, through the planned departmental technological change due in early 2015.
- As of 1 August 2013, Government Digital Services (GDS) are assessing a full technology infrastructure solution for the department. It is crucial that Cabinet Office establishes business requirements for the management of information and records at the heart of the project. This would be facilitated by the central involvement of the department's knowledge and information management (KIM) specialists in the new project.

Information risk, governance and oversight

Recognising information risk	**Development Area**
Setting direction	**Satisfactory**
Providing guidance	**Satisfactory**
Measuring impact	**Satisfactory**

- Cabinet Office places a strong emphasis on security and access controls. This may be the best platform for expanding the general understanding of information risk as staff already recognise requirements for the appropriate sharing of information. The Prime Minister's Office and the Cabinet Committee teams are exemplars of effectiveness in information management in high profile and pressurised environments.
- Clarity is needed over the information risk management approach within the department. The SIRO's leadership is vital to these activities. Information risks, including those relating to information management, need to defined, documented and managed corporately. Existing structures such as Information Asset Registers (IARs) and information risk and information security policies may be used to facilitate this. There would be a real reputational risk to Cabinet Office if it failed to fully demonstrate control and oversight in this regard.
- Cabinet Office's emphasis on securing and protecting personal information creates a tendency to over protect and restrict information 'just in case'. This is borne out in the Induction training. While some areas, such as Government Digital Services, have developed their own comprehensive local induction programmes, KIM and general records management is not included in the induction training as standard for new civil servants. The inclusion of KIM and records management in induction training is effective in encouraging staff to adhere to policy and promotes good practice in these areas from the outset. The movement of staff between teams also offers an opportunity to reinforce good practice principles and emphasise required ways of working including in relation to records management. Cabinet Office should particularly consider requirements for senior staff, given their ability to influence and determine corporate culture.

Records, review and transfer

Oversight of records and selection	**Good**
Implementing disposal decisions	**Satisfactory**

- The KIM Unit actively works to promote understanding of the importance of Cabinet Office's historical records. The team holds History Days to highlight Cabinet Office Records that have been released, which are supported through a series of ‘Behind Closed Doors’ pamphlets. Cabinet Office is currently meeting its obligations under the Public Records Act (PRA). Paper records are well managed and the department is up to date with reviewing files ready for transfer to The National Archives. The department has worked closely with The National Archives to resource the release of records, and to meet its obligations under the 20-year rule. Cabinet Office has worked to stagger the transfer of records ahead of press events arranged by The National Archives to promote the release of tranches of the department's records, in line with their profile.

- Cabinet Office needs to ensure this level of performance can be maintained over the next nine years, against on-going requirements for compressed timescales. To reduce the risk that deadlines may become harder to meet, Cabinet Office should put in place clear planning to fulfil future obligations. Applying this across all formats of records, including requirements for the disposal of extant and yet to be created digital records, would support Cabinet Office in taking the lead as a good practice exemplar for the rest of government.

Highlights table

The following table highlights areas of good practice identified at the time of the assessment. It includes systems and approaches that can be helpful in mitigating some of the potential risks to information that departments commonly face.

1	The KIM Unit hold regular History Days to highlight Cabinet Office Records that have been released, with a series of pamphlets titled ‘Behind Closed Doors’. These are a useful tool to demonstrate the importance of records keeping.
2	Government Digital Services has a comprehensive local Induction Programme that supports knowledge management.
3	The Prime Minister’s Office Correspondence Unit’s 10 Share is an impressive, well-managed electronic correspondence and email management system.
4	Cabinet Office’s What to Keep Schedule, and signed WTK Agreements are comprehensive and well thought out.
5	The KIM Unit processes for paper records, including sensitivity review, are well defined and well managed.
6	The Efficiency and Reform Group’s use of social media to publish policy and information updates is effective.
7	Cabinet and Cabinet Committee operate in pressured work environments, but have well-established and consistently applied processes in place that enable and support accurate and effective records management.

Recommended actions to address risk areas

Ref.	Summary recommendations
1	**Cabinet Office to reassert the value and importance of its Knowledge and Information Management (KIM) objectives in meeting departmental objectives.** This recommendation includes the need to: • Formally assess the benefit gained from the Information Strategy, and use this as a platform to reassert the importance of achieving its strategy goals. Formal senior-level support would help drive consistent practice in information and records management. • Develop a resource plan to ensure specialist KIM skills are available to meet future requirements. • Use the KIM Unit as support to Heads of Business to prioritise What to Keep (WTK) schedules for the policy areas that do not have them. • Tie in the production of WTK schedules with other departmental information gathering initiatives or projects as appropriate, such as Freedom of Information (FOI).
2	**Cabinet Office to create a support structure beneath Executive Management Committee (EMC) so that information management issues can be discussed in sufficient detail.** This **priority recommendation** includes the need to: • Establish an internally focussed Information Management and Assurance Group. • EMC to demonstrate support for Information management and assurance issues. • Agree a schedule of regular reporting to the EMC.
3	**Cabinet Office to strengthen its governance of Information Risk so the Senior Information Risk Owner (SIRO) has the assurance that the department is able to fully identify, mitigate and manage risks to its information.** This **priority recommendation** includes the need to: • Define how reporting structures can work together to support the SIRO in maintaining oversight and visibility of risks raised by information and records management, including capture and retention, and their potential effect. • Ensure that updates to the Information Risk Policy firmly establishes how Information and records management related risks should be tracked and mitigated within the organisation’s risk management framework.

	• Clarify the purpose and use of Information Asset Registers (IARs) to ensure consistency. • Refer to Digital Continuity Guidance to extend the scope of IARs beyond datasets, and to gain additional benefit from their use as a management tool. • Review and revise specific contingency plans for information stored on external information systems.
4	**KIM Unit to ensure that standards in Cabinet Office record keeping are maintained so that EMC has assurance that Cabinet Office's legacy is assured.** This recommendation would be supported by: • Defining how records management priorities can be promoted to new civil servants entering the department and to staff moving between teams. • KIM Unit defining options for strengthening KIM governance and oversight within the business and ownership of compliance by teams (via defined roles or other means) • Regularly review the roles and responsibilities of Information managers, record management staff and Information Asset Owners (IAOs) so that their information management responsibilities are coherent. • Developing KIM metrics to support oversight of performance and understanding of progress in managing risk. • Revising and updating the Information Retention Policy to include new ways of working such as Cloud-based storage and producing an appraisal report. • Developing plans to raise awareness and monitor adherence to key KIM guidance, such as Managing Records in Private Office and email policies. For example, Cabinet Office must ensure that requirements for audit and compliance are clearly identified as a component of the technology change project.
5	**Information and records management functionality must be integrated into business requirements for the technology change project from the outset of the project.** This recommendation would be supported by • Inclusion of the Head of Knowledge Management/DRO function on the Cabinet Office technology change project board once established. • Ensuring that business requirements for information and records management form the basis for more detailed functional and operational requirements (and user stories).

1 The value of information

1.1 Communicating and realising value

IMA Goal: The organisation establishes information's value in principle and supports the realisation of value in practice

Communicating the value of information

The Cabinet Office's February 2012 Information Strategy is closely aligned to the Information Principles. It is presented as the umbrella strategy for five key policies and strategies, covering retention and disposal, open data, information storage, and security and the knowledge management strategy.

The Strategy references the Information Principles for the UK Public Sector and recognises information as a valued asset that needs to be managed. It also references the Civil Service Code requirement to 'keep accurate official records and handle information as openly as possible within the legal framework.' It underlines the benefits of good practice in terms of legal compliance and managing the cost of keeping the information.

Although staff at all levels were clear on their departmental priorities and the responsibility to maintain a record they were either less clear about how to do this in practice or felt that the systems provided were burdensome. The Information strategy should be setting direction and influencing what information is stored and kept, and in what manner. Without clarity, direction and governance, staff may continue to make their own decisions on saving information on an individual basis according to locally defined priorities. The strategy is the opportunity to give direction and focus from senior management on the value of information. Cabinet Office should assess what benefit has been derived from the strategy and supporting policies to date. It should ensure that on-going focus is placed on gaining consistency in information management practice across the department and the support of senior leaders across the department. **See recommendation 1**

Establishing leadership and promoting value

Executive Management Committee (EMC) owns Cabinet Office's Information Strategy and aims to provide an overarching structure for all its information management-related policies. The Head of Finance owns and has board level responsibility for strategy. Day-to-day management of the Information strategy and prioritisation of issues is delegated to the Head of Knowledge Management.

Evidence of the effectiveness of current governance structures that support communication of priorities in implementing, managing and consistency of approach to information management-related policies was limited. There was also general confusion around the overlap between the roles and responsibilities of the Senior Information Risk Owner (SIRO), Chief Information Officer (CIO), Departmental Records Officer (DRO), Information Asset Owners (IAOs) and the Departmental Security Officer (DSO), and how they work together for the benefit of Cabinet Office's information management, information assurance and information asset management objectives.

Opportunities for these roles, to operate as a networked group were limited and localised. [1] For example, the DSO held regular internal meetings, with designated information security and assurance colleagues, but that is to discuss security relating to the infrastructure and physical security of the estate.

This lack of consistency and oversight of key information risks and information management issues contributes to a disjointed and incomplete view of information management within the department. As a result, KIM was perceived by a number of interviewees to be no longer a priority for the whole department.

[1] See Security Policy Framework for further guidance.
https://www.gov.uk/government/publications/security-policy-framework

In The National Archives' experience, best practice dictates that there should be an internally focussed group for information management and assurance. This would support Cabinet Office to assess impacts of external facing policy on the department, much in the same way as other departments do when faced with general Cabinet Office government wide directives. This group would need to meet regularly. The frequency should be decided in the light of departmental or interdepartmental change initiatives and technology refreshes, such as the department's anticipated 2015 information and technology refresh.

This group needs to act as the conduit to link information and records management and information assurance. The Chair should report to EMC. **See recommendation 2**

Enabling access to public information and supporting transparency

The Freedom of Information (FOI) team is located within the KIM Unit, under the responsibility of the Head of Knowledge and Information Management. The Cabinet Office has prioritised working with The Information Commissioner's Office to address FOI performance issues, response times and the consistent application of exemptions. In the period 1 January - 31 March 2013, Cabinet Office received 452 FOIA requests. [2] Of these requests, 86% were answered within time. Statistics published since the IMA was conducted show that performance dipped slightly for the following two quarters. Figures for the first quarter of 2014 indicate a higher volume of requests were received, with 95% answered within the 20-day deadline or permitted extension.

The upward trend since 2011 in performance noted with respect to the statistics suggests that prioritising FOI activity has had a positive impact. However, several interviewees expressed concern that prioritising FOI responses although positive in the long run, in the short term has had a knock-on effect on the KIM Unit's ability to promote awareness and

[2] Freedom of information statistics: Implementation in Central Government, January to March 2013 Ministry of Justice.

adherence to information management policy. Senior management have acknowledged that prioritising FOI has had an impact on the support and delivery of KIM services within the department. It was noted that most interviewees referred to the KIM Unit as the ‘FOI team’.

Currently there is a business case being presented to EMC looking at on-going priorities and resourcing within the KIM Unit. **See recommendation 1**

Publishing Information

The Minister for Cabinet Office leads the transparency agenda for government. Cabinet Office’s Open Data Strategy is governed by EMC. The strategy outlines what information is to be published and frequency of reporting. Evidence presented demonstrated that the Efficiency and Reform Group (ERG) has fully embraced open government and built their profile and reputation on the use of social media, utilising Twitter and blogs. ERG is an active publisher of information on data.gov.uk.

To ensure continued compliance with the Public Records Act (PRA) and Cabinet Office’s own policies, social media should be treated as part of the official record of Cabinet Office business. As such, a retention and disposal schedule created to determine what information needs to be kept and for how long. Guidance needs to be in place and followed to ensure that information is captured and stored within departmental systems as required by the Information Policy. **See recommendation 4**

1.2 Managing Information as a valued asset

IMA Goal: The organisation protects, manages and exploits its information as an asset to achieve maximum value

Knowing what Information exists

Interviewees describe Cabinet Office as a ‘dynamic’ and ‘fast-paced’ department that is constantly reacting to, developing and implementing changing government priorities. This is the working environment of Cabinet Office and should not be deemed a barrier to Cabinet Office retaining its legacy, but be recognised as the working culture of the department.

Integral to the cultural identity of the department is the relatively small core of civil servants, with many secondees or contractors working short term on specific policies or initiatives. This generates a situation where annual staff turnover is approximately twenty per cent, making achieving and maintaining good information and records management practice all the more vital.[3]

The inherent pressures of the work contribute to how information is valued. The speed of policy delivery required and the requirement to achieve, mean that often, information is used for the task in hand with little thought on the residual value of the information beyond first use. Therefore, information is seen as a local and not a global departmental asset. The onus is on the department to ensure that they have a means to safeguard key legacy records in whatever format. Cabinet Office must develop innovative and pragmatic ways to keep its records when it is subject to a dynamic and fast-paced environment. The forthcoming technology refresh provides an opportunity to incorporate information management requirements. **See recommendations 4 and 5**

Defining and recognising information is an asset

Corporate governance of information assets was not clear to the assessment team. There was some direction regarding information asset management within the department. However, there was no overarching management approach for information asset management within Cabinet Office.

There was confusion over who had overall responsibility for information asset management, including the lead on completing the IARs. Various responses to the question were ‘Security’, ‘the Estates team’ or ‘the KIM team’. A previous incarnation of a formalised executive level reporting structure was

[3] Cabinet Office HR figures –September 2013

the Information Assurance Board; however, this had a pan-government remit and was not internally focussed on Cabinet Office. **See recommendation 3**

Staff interviewed stated that priority is given to documenting key information systems within Information Asset Registers (IARs), together with minority datasets and personal information in general terms. The emphasis was found to be on securing and protecting information.

The assessment team was only able to view one local example of an IAR and was therefore unable to assess overall standards despite requests. However, several senior interviewees conceded that the understanding of information assets was ‘patchy’. Evidence was presented of standalone PCs and databases although recognised as repositories for business information had not been formally identified as an asset, and therefore not been added to an IAR. This raises concerns over the consistency with which the department’s approach is currently being communicated and applied.

An IAR can provide oversight for non-personal as well as personal information. It can be used as a tool to enable the exploitation of information by defining business value, purpose and capturing potential future uses. It can also encompass unstructured as well as structured information and enable understanding of the relationship between information and supporting technology.

Cabinet Office holds few very large datasets and the department’s use of IARs reflects minimum requirements of its own guidance published under the Security Policy Framework and risks specified within the Information Strategy. However, Cabinet Office could be gaining more benefit from its IARs as internal management tools that support the management, exploitation and reuse of its information and ultimately making more information available to citizens. This approach is exemplified both in the Information Principles for the UK Public Sector and in guidance produced by The National Archives’ digital continuity project, of which Cabinet Office was a key sponsor. Ensuring that value is consistently defined and captured would also help the department ensure it is safeguarding its information assets as set out in the information security policy. **See recommendation 3**

Ownership of information assets

Where information assets have been defined, first-tier ownership has been assigned through IAOs, the majority of whom were Heads of Business (HoB). Appointing IAOs at HoB level is **a positive move**. It gives a sense of importance, responsibility and priority to the role. However, the reality for HoBs having other departmental responsibilities and pressures meant that a number of HoBs did not access training, increasing the risk that the department is not fully compliant with all aspects of Mandatory Requirement 1 of HMG Security Policy Framework.[4] **See recommendation 3**

To demonstrate good internal governance Cabinet Office will need to ensure that the information asset management process is effective. Cabinet Office would benefit from introducing its own internal information awareness sessions initially, with a suite of guidance targeted at HoB level. Formal SIRO and IAO training is also provided by The National Archives. **See recommendation 3**

[4] HMG Security Policy Framework Mandatory Requirement 1
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf

2 Information and supporting technology

2.1 The technology environment

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

Managing digital Information

Digital information is shared across a number of platforms that are not interoperable. This is a result of machinery of government changes, inheritance of legacy systems and differing security requirements. The department has two different Electronic Document Management Systems (EDRMS): Meridio and Retriever, which are both used to varying degrees. A minority of staff also have access to another system for more highly classified information. The KIM Unit provides limited support on the use of the EDRMS when requested. Effective use of the EDRMS would have allowed Cabinet Office to support full life cycle management of digital records.

Shared drives are also available in the majority of the business areas. Interviewees explained that there are several reasons why shared drives were created, such as to store databases or information that would not readily fit into either EDRMS. Several interviewees stated they used shared areas in preference to the EDRMS as it was easier to keep information ‘close at hand’ and accessible due to concerns about finding information once stored in the EDRMS. This is further complicated by shared drives being managed by the ICT contractor Fujitsu as part of the shared ICT arrangements with Her Majesty’s Treasury (HMT). The KIM Unit can view but not control the file structure. **See recommendation 4**

An increasing risk for Cabinet Office is the lack of retention schedules on its digital systems. This has created a large repository where information is added to without a plan for when and how this information will be reviewed and disposed. One interviewee described this as the ‘big bucket’ approach as ever-increasing information is added to systems with no end date. The lack of a retention policy raises the risk that as more information is added to systems, it will become harder to find it and make it available. One senior manager commented that not handling information effectively leads to a, ‘slow burning serious problem in the future’.

Cabinet Office needs to assess how it will manage this situation. Clearly, the feasibility of doing a retrospective application of retention schedules may not be practical. However, without clear evidence that this issue has been highlighted and escalated to EMC as a core information risk with mitigating actions, then Cabinet Office may not be managing its information and safeguarding its legacy consistently across the whole department.

Cabinet Office has the ability to address this through the anticipated major departmental technology change scheduled for early 2015. Under the Public Records Act, the department needs to identify which information needs to be kept for historical preservation. In order to do that, Cabinet Office needs to know what is in its digital systems. An appraisal report would help identification of information of value and the legacy digital collection needs to be managed in line with it, with information that is not needed for historical preservation, deleted when no longer needed for business purposes. **See recommendation 4**

2.2 The Continuity of digital Information

IMA Goal: The organisation is taking proactive steps to assure the continuity of its information over time and through change

Considering digital continuity ahead of change

At the time of the assessment Cabinet Office had been in the first stage of implementing a joint IT project with HMT, called Infostore. This entailed the use of Windows-based SharePoint software to provide a means of better information and records management and to act as a vehicle for collaborative working. Infostore was piloted in Property Services while the assessment team was on site.

The assessment team had concerns about the project rollout within Cabinet Office, timescales, project support and communications within the department. The main issue was the tight timescale between the rollout of pilots and scheduled departmental implementation of three weeks. The assessment team identified a clear risk that if there were any major technological issues found within the pilots, there would not be enough time to address these. A presentation to EMC on lessons learned and progress of the pilots was scheduled for 1 August 2013.

The National Archives understands that EMC decided to halt the project immediately as it was proving problematic and concerns were expressed about the long-term suitability of Infostore to meet Cabinet Office requirements. As a result, Government Digital Services (GDS) have been tasked with assessing and developing plans for a full technology infrastructure solution for all of Cabinet Office effective from early 2015.

As well as improving the technological infrastructure, this development has the potential to resolve several of the information management issues raised within this report. It is recommended that the Head of KIM/DRO function is represented on any subsequent project board to ensure that the development of information management requirements is integral to any solution. **See recommendation 5**

Consideration also has to be given to ensure that Cabinet Office's information stored on systems that are managed by external parties, such as Fujitsu or Google, is fully retrievable. Cabinet Office must have clear contingency plans that outline the circumstances, timescales and expectations should all Cabinet Office information be required to be removed in full. **See recommendation 3**

3 Information risk, governance and oversight

3.1 Recognising information risk

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

Creating the right culture

Cabinet Office understands information risk in general terms. Staff understand the risks implied by failure to protect information and staff work hard to ensure that information is not shared inappropriately. The emphasis is on strong security and access controls. This is **a good base** on which to expand understanding of information risk. There are some examples of good practice, such as WTK schedules and appropriate use of corporate repositories. The Prime Minister's Office and the Cabinet Committee teams are also exemplars for what can be achieved within a high profile and pressurised environment.

Implementing an information risk management approach

The department has the responsibility of being the lead on information assurance and information security for government. Cabinet Office already has senior officers internally who understand information risk and has the ability to define, mitigate and manage risk on a large scale. The absence of a support structure below EMC has made implementing a risk management approach difficult for the department. **See recommendation 2**

Whilst it is meeting its external government remit, Cabinet Office needs to ensure that it can fully demonstrate how it manages its own information risks at all levels.

It is imperative that the SIRO leads information risk activities for the department and fully engages with and uses the support of the departmental CIO, DSO, Head of KIM, Information Managers and IAOs to provide cohesion and consistency. **See recommendation 2**

Cabinet Office has the potential to make full use of its IARs to support the identification, location and mitigation of risks that all contribute to the effective management of information. Over time, this will permeate throughout the department. **See recommendation 3**

Documenting and defining information risks

Cabinet Office's information risk approach is focused on securing information and on data protection. This is understandable given the political sensitivities of certain functions, and is heightened by the incoming departmental responsibilities in relation to the electoral register. However, the assessment team is pleased to note that the department's 2012 information security policy recognises the Public Records Act among the significant legal and regulatory requirements placed upon government departments. The policy also defines the role of the Head of KIM in ensuring records compliance. The separate information risk policy also makes a strong and statement that, 'Poorly managed information can lead to a material impact on an organisation; financially, reputationally and even legally.' The policy underlines the need to dispose appropriately of information and data when it is no longer required.

There was general understanding among staff that the biggest consequences of not managing information effectively were: being unable to respond to Ministers; being unable to fulfil FOIA requests; 'double handling' information; and not being able to trust the authenticity of information when needed for policy development or decisions.

The effect of these risks is recognised within the business. To support delivery of its Information Strategy, Cabinet Office should build on the foundations already in place and ensure that information and records management related risks in particular are defined, captured and communicated at the right level. The assessment team did not gain full assurance that this is happening currently. The team recognises that information risks are captured by the KIM Unit and a separate IT risk register is maintained, but effort is required to coordinate information risk for the department. Several senior management interviewees recognised that they might not have a full picture of how information risk is managed within the department. They were relying on being told what the situation is, rather than relying on a formalised information risk reporting structure.

Cabinet Office has to improve this situation and raise its assurance levels. The risk remains that full assurance cannot be given due to the lack of a rigorous evidence base. The recommendation for SIRO engagement and full internal information risk governance will support this. Cabinet Office plans to conduct a review of corporate policy to coincide with its IT refresh. It should take this opportunity to establish through its Information Risk Policy how information and records management related risk needs to be documented, monitored and mitigated. **See recommendation 3**

3.2 Setting direction

IMA Goal: The organisation has effective governance structures for information in place that foster communication and planning

Governance and planning

Appendix C of the Cabinet Office information retention policy describes the core information management responsibilities of the DRO, Head of Management Unit, Information Managers and staff in general. As an existing departmental resource, Cabinet Office should define how these roles will be used to support the department's KIM agenda and where necessary support the information risk management approach as it develops.

There will be benefit in linking these roles and responsibilities to other KIM and records management policies so they are seamless and well rounded. For example, common objectives and responsibilities related to the information management strategy and Information policy for the department will help reinforce and provide consistency. This has added relevance to the anticipated changes in departmental ICT projects. **See recommendation 4**

The benefit of this approach would be to ensure that the EMC is informed on information management and then able to make timely decisions in the knowledge that internal governance within the department is working, and working well.

3.3 Providing guidance

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

Guidance and training

All staff interviewed stated that they had completed the mandatory data protection and security e-learning. A high percentage fully understood their obligations stemming from the training, regarding data protection and securing information.

Staff acknowledged that in some areas, the emphasis on security and protection of personal information resulted in a tendency to over protect and restrict information 'just in case'. The revised and simplified Government Protective Marking Scheme (GPMS) is due to be launched by autumn 2013. Cabinet Office should review how GPMS is communicated once the new scheme is available. This should be linked into new or emerging information technology infrastructure and change projects, promoting a consistency of message and a wide understanding of the appropriate use of the new GPMS. **See recommendation 4**

The mandatory e-learning is a requirement of the induction process into the department. The central training is provided by Cabinet Office HR. Knowledge and information management and records management are not included in the training. As staff are introduced to Cabinet Office standards on securing and protecting information, training is needed for IM and RM. Induction provides an opportunity to set the benchmark as staff new to the civil service join the department, and to reinforce standards through the line management chain when staff change teams. For new entrants, it is the most effective way to ensure that staff adhere to policy, use systems effectively and promotes good information management practice from the outset. The KIM Unit should capitalise on the opportunity and develop an information and records management element for the induction programme. **See recommendation 4**

Management of Private Office is an important function in any department. Interviews with various Cabinet Office Private Office (PO) staff illustrate the inconsistencies that can result without a clear corporate mandate for KIM. Each PO contained dedicated and conscientious staff who understood the requirement to ensure a record of departmental and Ministerial business was kept. Some had formal written guidance and others had verbal instructions and shadowing as their induction. Staff were themselves confident that important decisions or conversations were fully captured.

However, there was a lack of certainty over whether the originating policy area or business area was responsible for keeping the record if a Minister or senior civil servant commented on a key document. This led to instances of keeping the information in PO as well as within the policy areas. The risk is either that information is double handled or that a lack of clarity means that copies are deleted by policy areas and PO.

A level of appropriate standardisation on working practices is required across Cabinet Office if the ambition is to be the ‘best private office in Whitehall’. Clarity is also needed about which private office model is to be followed enabling a more consistent approach across policy areas and POs and to support future selection and sensitivity review. **See recommendation 4**

Knowing What to Keep

What to Keep (WTK) was piloted within Cabinet Office in 2010 and its WTK strategy is called ‘Managing Information’. The strategy is well-defined and comprehensive. It also makes clear the need to prioritise core information and also to delete information when no longer needed. The KIM Unit had worked extensively with departmental Heads of Business to get the majority of WTK agreements secured. The individual signed WTK agreements could be used as **a best practice** example across government. The complexity and diversity of the WTK schedules illustrate the priority given to achieving this objective.

Since 2010, several WTK schedules have not been updated nor have any been created for newer policy areas. In the context of the high staff turnover and the pace of business change it is especially important to establish these; particularly in areas that are already using non-standard information systems, such as GDS, who are using cloud-based information management solutions.

It is important that emerging policy areas are supported through provision of WTK schedules and guidance. Priority should be given to completing them. WTK schedules need to be relevant to the work environment and must ensure that the legacy is assured with key decisions kept. It is vital that Cabinet Office is able to retain the right information, secure in the knowledge that it has a complete a legacy as possible. **See recommendation 1**

The assessment team is not advocating that Cabinet Office develops another separate exercise for WTK, as this may not be the most productive or time efficient route. Rather, it should be looking at innovative ways to tie in completing schedules with other departmental priorities, such as the on-going work in raising the performance of FOI and capitalising on established networks and contacts. This will give the double reassurance that core information is being saved in a structured way and that information that may need to be disclosed under the Freedom of Information Act (FOIA) is available.

Email and records management

Cabinet Office must enforce its email policy and be clear on staff responsibilities when using departmental email. Staff’s ability to archive and create personal storage table (PST) files from the email accounts presents a clear information risk to the department. One interviewee did admit to having archived 20,000 emails in PST, and while others also had several years’ worth of files that only they could access. Interviewees recognised this was not best practice or good information management but felt that this was justified as this was more reliable than placing information in corporate repositories.

Cabinet Office has recently introduced an email policy specifically for the use of private email accounts to address concerns that staff are not ensuring that business information is accessible and stored in corporate systems. It is too early to assess the effectiveness of this policy.

In a department where there is a formal information and records management governance structure, this would not be so much of a challenge. As Cabinet Office's KIM governance is patchy, it is likely that core business information will remain inaccessible within personal email accounts.

3.4 Measuring impact

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

Assessing progress against strategic goals

The Department has found it difficult to align with strategic KIM objectives, or assess progress against them. The cancellation of the Infostore project and the anticipated technology infrastructure changes makes this the ideal opportunity to both review and align policies beneath the Information Strategy to provide much-needed cohesion, direction and focus.

Measuring compliance with policy

Another complication to the effective management, protection and exploitation of information within Cabinet Office, is the divided responsibility for managing the EDRMS and shared drives. It makes the production of management information or suitable KIM metrics on system usage difficult and unwieldy.

Regular reporting of accurate management information and KIM metrics provide visibility of system usage and has been used by other IMA participants to raise the profile and increase use of corporate information systems, such as EDRMS or approved file plans. The National Archives recommends this approach as part of the revised KIM governance arrangements. **See recommendation 4**

Appendix B of the Cabinet Office's Information Retention Policy recognises the Cabinet Office compliance with legislation and codes of practice. Other than compliance with FOIA, it is difficult to gauge other compliance within Cabinet Office without a clear strategic view. The overarching requirement is to have assurance that the department is meeting its obligations. The current limited KIM oversight does not lend itself readily to this. Existing governance arrangements, such as internal audit or the recommended information management and assurance discussion group, should be used as tools to achieve and support compliance. These structures can be multidisciplinary and can work laterally across the organisation.

The assessment team recommends the KIM Unit should capitalise on existing governance arrangements to reinvigorate the KIM professional network, by reassigning Information Managers and utilising IAOs and records management staff. **See recommendation 4**

The National Archives acknowledges that this will not be an easy task. Cabinet Office is obliged to manage its knowledge and information efficiently and effectively and in doing so retain its important legacy. The risk facing Cabinet Office is that without an active and supported KIM strategy and up-to-date WTK schedules, the future legacy of the department will be compromised.

4 Records, review and transfer

4.1 Oversight of records and selection

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

Compliance with the Public Records Act

Cabinet Office's Information Retention Policy is a comprehensive document that clearly states Cabinet Office's obligations under the Public Records Act (PRA) and other legislation. It is owned by the Head of KIM as DRO for the Cabinet Office and the Prime Minister's Office. Cabinet Office has worked hard to ensure that it is meeting its obligations under the PRA and is confident that it has a well-managed, well–developed, competent process for paper records.

The risk is that recognising the importance of good information and records management practice has lessened with regard to digital information, making it necessary to increase efforts to raise understanding of an appropriate records management standard. This reinforces the importance of having consistent and effective internal KIM governance to give oversight and ensure that one initiative, such as prioritising FOI, does not compromise another.

Managing resources and 20-year rule transition

The latest Record Transfer Report (RTR),[5] May 2013, shows the level of outstanding records to be reviewed for transfer to The National Archives.

Appraisal and selection

Cabinet Office has four reviewers. Two part-time reviewers are assigned to reviewing the Prime Minister's office files and the other reviewers review the rest of the department. This makes Cabinet Office vulnerable if that member of staff is unavailable especially in the context of other KIM priorities regarding

[5] http://www.nationalarchives.gov.uk/about/record-transfer-report.htm

FOI requests directed at the archive. Cabinet Office should assess the risks around future resourcing for such an important role, especially when placed in context of the other pressures within the KIM Unit and that the requirements to meet the 20-year rule transition have doubled the annual output.

There is also the potential risk that knowledge within the KIM Unit will not be available. It is recommended that there is a clear succession plan with a training programme to minimise disruption to the function. **See recommendation 1**

The KIM Unit has demonstrated that it can encourage good records management by engaging staff on historic records with their preview days of records that are about to be transferred and opened at The National Archives. The series of Behind Closed Doors leaflets were produced. These are viewed **as good practice**.

As the governance structure for KIM is reinvigorated and communicated the KIM Unit should continue to encourage good records management by using recent activities, e.g. the planning of the funeral of the former Prime Minister, to demonstrate the potential benefits of good present day information and records management on the department’s future legacy.

4.2 Implementing disposal decisions

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

Sensitivity review

The system for paper review is well established. Sensitivity review is carried out on a file-by-file basis. Cabinet Office are currently up to date with reviewing files ready for transfer to The National Archives but this is due in part to the fact that they were ahead of schedule for 2012. This performance has enabled Cabinet Office to keep pace with 2013 work.

Government departments preparing records for transfer to The National Archives should review the access requirements of those records, irrespective of format. Cabinet Office needs to review future resources, including the skills required to meet government targets in the transition to support the move to the 20-year rule and the need to make decisions on digital records draws closer. To develop understanding of challenges raised by sensitivity review, Cabinet Office should ensure that it engages fully with The National Archives digital transfer project. This includes taking the opportunity to participate in a pilot transfer of a defined set of records. **See recommendation 1.**

Disposal and planning to transfer

At the time of assessment, the latest Record Transfer Report (May 2013) records Cabinet Office as having over 8000 records awaiting review or a decision on transfer within 2013. A view as to how many of the files will be accessioned to The National Archives is expected shortly.