The National Archives

Information Management Assessment

Foreign and Commonwealth Office

August 2010

October 2009

PART ONE: EXECUTIVE SUMMARY

Executive Summary

1. Information is critical to the business of the Foreign and Commonwealth Office (FCO), and hence effective information management is key to the Department's ability to make important decisions each day based on its information. In the view of the Assessment Team, FCO often focuses on using information for its immediate benefit, and less on maximising its wider value to the Department. The Assessment highlighted some risks and issues which when addressed will ensure that FCO can make best use of its information across all its business.

2. FCO has recognised the need to change and has started to make some progress. Positive changes include the introduction of the i-Records system, development of a Knowledge and Information Management (KIM) strategy and re-issuing of policy and guidance. These are progressive steps which when fully implemented and communicated will enable FCO to manage and exploit its information more effectively.

3. Whilst information assurance has been given a high priority within the Department, more effort is needed to assess fully the wider risks to good information management. Information risk in its widest sense – including risks to integrity and availability – should be the guiding principle, not just an interpretation of information risk as information security. This means embedding good information management practice in the business. FCO has started tackling the HMG Information Assurance Maturity Model and Assessment Framework (IAMM) focused on protecting electronic information including personal data, but the Assessment Team identified opportunities for improvement in the Department's management of wider information risk. For example, FCO needs to be confident that it is managing the risk of not retaining the evidence of key decisions or of failing to share critical information across the organisation or with key partners. The Assessment Team evidenced recent examples where it has been difficult for the Department to find its information in response to external requests, and

where the inability to find it could have carried reputational risk. This should prompt FCO to reassess its evaluation of information risk.

4. Governance is vital to ensure that information is both fully managed and exploited. At each level, people need to know what their responsibilities are and how information can help them in their work. A clear steer and support from the top is essential in achieving this aim. The benefits of good information management practice are plain - delivering well informed decisions, enhanced efficiency and mitigation of risks. In some cases, insufficient clarity and guidance has led many staff to develop local practices and not view information or information management as a priority. For example, the Assessment Team found examples of staff using their own record and information systems, being unsure about what information to keep and displaying inadequate and inconsistent use of records management software.

5. In making best use of its information, FCO has to contend with many challenges, including intense pressure to make quick decisions, a dispersed workforce, staff rotation and a staff based both in the UK and overseas. There are areas of good practice, such as the information management practices of the Research Analysts and the management of high classification records, but the Department could improve its co-ordination on these issues. The Assessment team found it difficult to establish a sense of corporate memory, or a record of FCO as a whole in relation to digital records. Additionally, without improvements to knowledge transfer in a Department that frequently rotates staff, there is a significant risk of loss of legacy knowledge.

6. FCO handles some aspects of its paper information extremely well, with thorough audit trails providing good quality information. The advent of the digital age has caused some decline in how well information is being kept within FCO, which can make it difficult to access and recover documents. Although there are areas of good practice, such as FCO's treatment of high classification material, the picture is not consistent. Many staff, without clear governance or guidance, have developed elements of poor practice over recent years.

7. The structure of the Information Management Group limits effective support for good information management. For example, records and information management practitioners are separated from information

storage. Furthermore, there is an available records management resource based in Hanslope Park which currently only considers paper records.

8. The assessment highlighted the fact that FCO has until recently viewed its IT systems and the information held on them as separate functions. The focus has been on getting the global infrastructure and platforms right, which is understandable. Many of the information management initiatives in recent years have been poorly resourced and supported. There is a now an opportunity for the FCO to address this. It is vital that IT and KIM work alongside each other, and that information audits carried out by FCO are seen as an important tool in ensuring good use of the IT systems. The information audit role could be expanded to cover a more comprehensive approach to information management, including communications and training. This is a challenge shared by all Departments.

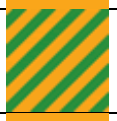
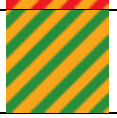
9. FCO needs to define more clearly which of its information assets have business value. The KIM strategy should inform and determine exactly how FCO will manage its information and knowledge assets. Once FCO is certain about what it should keep, it should then consider how the information should be kept. The risk of losing, of providing inadequate protection for, or not being able to find, core business information or records of key decisions is both significant and substantial, not least because the volume and complexity of FCO's digital information and data holdings keep rising inexorably.

10. The widespread sharing of knowledge and information is not yet at a mature level within the FCO. There is no codified system to help staff share the information they hold, or to ensure that knowledge is transferred consistently when staff move from one post to another. This is a real risk in a Department that frequently rotates its staff, and could lead to decisions being made without access to the full facts, duplication and a lack of efficiency if information is not easy to find, or, its actual existence is unknown. There is anecdotal evidence that, in some cases, staff are still keeping corporate information in personal drives and this is simply destroyed when a staff member moves on.

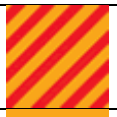
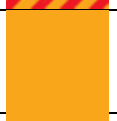
11. This assessment has highlighted areas that FCO should address to ensure that it continues its progress in becoming more effective and efficient in managing its knowledge and information to achieve its overall business objectives.

Risk Matrix

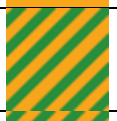
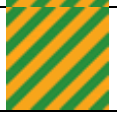
Governance and Leadership

Strategic management		Satisfactory
Business objectives		Good
Management controls		Satisfactory
Resourcing		Development needed
Risk management		Good

Records Management

Creation		Development needed
Storage		Satisfactory
Appraisal, disposal and transfer		Satisfactory
Sustainability of digital records		Satisfactory
Management		Development needed

Information legality

FOI/Data Protection		Satisfactory
Re-Use		Good
Security		Good

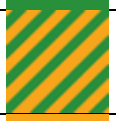
Compliance

Staff responsibilities and delegations		Satisfactory
Policies and guidance		Satisfactory

Training		Development needed
Change management		Development needed

Culture

Commitment		Satisfactory
Staff understanding		Development Needed
Knowledge Management		Development needed

Key to Colour Coding	
	**Best Practice**
	**Good**
	**Satisfactory**
	**Development Needed**
	**Priority Attention Area**

PART TWO: INTRODUCTION

Information Management Assessments

12. The Information Management Assessment (IMA) programme is the best practice model for government Departments wishing to demonstrate a high level of commitment to managing their information. The assessment process ensures that government Departments meet the required standards for effective collection, storage, access, use and disposal of information. The IMA programme:

    - enables the Head of Profession for Knowledge and Information Management (KIM) to assess the effectiveness of the function in Departments;
    - sets out the capability of Departments to meet their KIM challenges and obligations;
    - assures the accounting officer that Departments are equipped to deliver their information management responsibilities; and
    - helps Accounting Officers plan for future information management developments.

13. The National Archives leads information management across government. The IMA Programme is a key element of that function. The programme's goal is to deliver measurable improvements in information management across government by providing robust, independent validation of the standards and integrity of the information management processes and capability within Departments.

14. The IMA Programme is aimed at core government Departments. To be admitted to the Information Management Assessment programme, an organisation will:

    - make a public commitment to the IMA programme; and
    - see the commitment successfully independently verified.

15. Once a Permanent Secretary or Chief Executive has declared the commitment, the underlying administrative and decision-making processes of the organisation are examined to verify that they support the IMA commitment.

16. This report sets out the findings, conclusions and recommendations of The National Archives' IMA Assessment of the Foreign and Commonwealth Office (FCO).

The Business of the Foreign and Commonwealth Office (FCO)

17. The Foreign and Commonwealth Office (FCO) currently employs 14,900 staff. 2,600 of these are employed in the United Kingdom. 12,300 are employed in over 170 countries throughout the world. FCO has 140 embassies and High Commissions, with an additional 102 consulates worldwide.

18. FCO also has 21 delegations and representations to the United Nations, the European Union, North Atlantic Treaty Organisation (NATO) and other international organisations. In larger posts FCO staff work alongside partners from other UK government Departments.

Current Departmental Strategic Objectives:

- Flexible global network serving the whole of the British government;
- Supporting the British economy;
- Supporting British nationals abroad;
- Supporting managed migration for Britain;
- Countering terrorism and weapons proliferation and their causes;
- Preventing and resolving conflict;
- Promoting a low-carbon, high-growth, global economy; and
- Developing effective international institutions, above all the United Nations and European Union.

19. The nature of FCO work requires close co-operation with other government Departments. The United Kingdom Border Agency (UKBA), Ministry of Defence and Department for International Development have large numbers of staff in FCO posts. This is not exclusive as other departments also have staff working within FCO posts abroad.

20. As part of the 2007 Comprehensive Spending Review (CSR07), the FCO aims to achieve at least a 3% annual cash-releasing Value for

Money (VfM) saving by 2010/11 on its 2007/8 Departmental expenditure limit baseline. In the 2009 budget, further efficiency savings targets were announced as part of the wider government drive to deliver an additional £5 billion in savings in 2010/11.

Information Management at the Foreign and Commonwealth Office (FCO)

21. FCO has in place a structure for information and records management. It is headed by the Chief Information Officer (CIO), who is also the FCO Board's Senior Information Risk Owner. The CIO heads up the FCO's Information and Technology Directorate (I&TD) which is spread across 2 geographic locations (two buildings in London and two in Hanslope Park - near Milton Keynes).

22. I&TD has an information and records management 'centre of excellence' called the Information Management Group (IMG), responsible for knowledge and information management, diplomatic bag policy, information risk and data handling, records management, information rights and historians. IMG works with the Information Management Officers (IMOs) and Open Government Liaison Officers (OGLOs) in each Directorate/Post.

PART THREE: ACTIVITIES CARRIED OUT BY THE ASSESSMENT TEAM

Methodology

23. The purpose of the assessment is to establish whether the key elements of the FCO's commitment to the IMA programme and their own Information Management (IM) priorities are achieved. A range of standard processes, systems and documentation were examined to determine if this was the case. This approach was based on a matrix model, as shown below, which takes essential business outcomes, and shows how work in each of the areas of activity demonstrates compliance.

24. FCO is divided into a number of key business and policy areas, relating to how the organisation is managed, governed, its vision and key business objectives, especially pertaining to information management. Key services across the range of FCO business groups were assessed into areas of assessment focus. The key business areas were considered according to a risk assessment carried out prior to the on-site visit. This was based on:

    - the findings of the pre-assessment questionnaire;
    - previously identified strategic risks; and
    - information management or skills issues identified in pre-assessment documentation supplied by the FCO themselves.

    The key business areas, and the areas of assessment focus, fall under the following headings:

Business Area	***Assessment Focus***
Governance	• Strategic direction, business objectives and performance indicators • Management controls • Capability • Risk management • Data Handling Processes

Records Management	• Creation, storage, appraisal, disposal, transfer, security, management and sustainability of digital records
Information Legality	• Access to and re-use of government information • Websites and equivalents
Compliance	• Staff responsibilities and delegations • Policies and guidance • Intranet • Skills/Training • Effects of changes in government policy or legislation
Culture	• The commitment to effective information management • Staff understanding of information management risks • Application of Policies and Guidance • Knowledge Management

Activities Undertaken

25. The Assessment took place from 28/09–02/10/2009. The Assessment Team:

    - examined key policy and practice documentation relating to training, skills and processes;
    - interviewed staff members from across the organisation;
    - tested the processes used; and
    - reviewed the website and intranet.

    These activities are described in more detail below.

Documentation review

26. FCO provided documentation in support of their information management objectives and the IMA commitment, which was reviewed prior to the on-site assessment.

People and Practices

27. The Assessment Team interviewed a range of staff at all levels, both nationally and internationally, who are involved in policy making and the interpretation and practice of managing information. These interviews were used to determine how people in the organisation work

and the impact of information management upon them.

Process Testing

28. A sample review of the day-to-day business processes was used to identify possible procedural gaps. This included electronic records management systems, retention schedules and general guidance and working instructions.

Intranet review

29. A review of FCO's Intranet was carried out to assess ease of use, utility of the information contained on it and to determine how up to date it was.

Website Review

30. A review of the organisation's website was conducted to establish the transparency of information relating to Freedom of Information, Data Protection, contact details and complaints procedures.

Risk Assessment

31. The Department's risk framework and associated information statements and policies were assessed to ensure information, knowledge and records management compliance.

Data Handling

32. The National Archives were joined on the assessment by colleagues from Information Security and Assessment within the Cabinet Office, which has the lead on information risk management policy across Government.

The Assessment Team

33. Each IMA is carried out by the Standards Team within The National Archives, with a team of external reviewers assembled to meet the requirements identified in the pre-assessment planning. The team comprised:

- Standards and Assessment Manager
- Head of Standards

- Information Management Consultant
- Standards Adviser
- Digital Continuity Manager

Assistance provided by the Foreign and Commonwealth Office

34. The Assessment Team are grateful for the co-operation and assistance of all staff interviewed, and especially the Information Management Group.

PART FOUR: HIGHLIGHTS AND AREAS FOR IMPROVEMENT

Governance and Leadership

> "I will provide effective leadership on Knowledge and Information Management capability across my Department." [Peter Ricketts]

Strategic Direction

35. In September 2009 Information Management Group (IMG) outlined its Knowledge and Information Management (KIM) Strategy to the Assessment Team and other colleagues in I&TD. IMG anticipates the strategy will raise the profile of KIM within the FCO. The strategy recognises that a cultural shift is required to ensure best use of its information and information systems, and also to ensure a coordinated approach with overseas staff. The creation of a strategy is welcomed.

36. In approving the KIM strategy, the FCO will need to consider its structure to ensure it gives full support to effective knowledge and information management. Without this, there is a risk that FCO will not be able to fulfil the commitments stated within the strategy.

37. The Assessment Team found that the understanding of knowledge and information management was variable across FCO. Strategic direction on what constitutes good knowledge and information management practice and standards within the context of the FCO needs to be restated and widely disseminated. The lack of clarity in relation to strategic direction could have a negative impact on the level of importance the department attributes to knowledge and information management and how this could impact on the business.

38. FCO, like other government departments, has ensured that information assurance is a priority for the Department. FCO now needs to progress the good work already done on information assurance focussing on protecting electronic information, and demonstrating the same high level commitment to information management that has been given to information assurance.

39. The FCO also needs to demonstrate that the Board are committed to information management and need to ensure that this message is communicated. This needs to be in tandem with the drive to raise

understanding and accountability for information management.

Structure

40. The Assessment Team found that there are areas of good information management practice and understanding within FCO, but often these operate mostly within functional silos. For example, management of paper files, the development of KIM and public diplomacy (where the use of social media is key) all work separately. There is a risk that without a coherent information management structure the FCO will not be able to capitalise on the good work already undertaken, and will be unable to raise the standard of information management across the board. The first stage in this structure is to ensure that there is a high level body that has responsibility for the strategic direction for KIM in FCO.

41. The Assessment Team have been advised that the FCO Board has recently created an IT Committee. The Assessment Team believe that incorporating the strategic governance of information management at this level would provide the high level focus and visibility that KIM in the FCO needs. With the creation of the strategic KIM-focused team, FCO must ensure that it sets out clearly for staff how systems are used, who is required to use them and what information is to be kept. This should be underpinned with the support of relevant policies, guidance and protocols. The long-term consequences of not doing this would be duplication of effort, lack of corporate memory, poorly evidenced decisions and a lack of consistency and focus.

42. FCO has already demonstrated with the information assurance programme that it has the will and the ability to raise awareness, gain commitment and drive information-related change in the Department. There is high level leadership, with accountability and visibility, for the comprehensive IT refresh and implementation of a new records system that is presently happening. The high priority and resources available to the programme were evident to the Assessment Team. A well managed and structured information management programme as a key part of I&TD's ICT strategy would do much both to support the ongoing IT system upgrade programme, and clarify the business drivers for it, by ensuring that information management is considered in a timely and coherent manner. This level of priority and visibility would do much to

push the wider information management agenda across the FCO.

43. While the Information Management Group brings together most aspects of information management, the intranet (FCONet) and extranet (FCOWeb) as well as Legal Library, Consular and other information management activities in the wider FCO sit outside IMG's governance. The Assessment Team found that the Consular Team had its own Head of Information Policy. IMG should be at the heart of any new IT development and needs to be recognised as the policy lead for information management and policy for the FCO as a whole.

44. In addition, the Information Asset Owners (IAO) do not currently have IM objectives as part of their overall business objectives. Although the Chief Information Officer is also the SIRO and has overall responsibility for FCO information assets, as well as being a member of the Board, the lack of a coordinated and coherent approach to information management throughout the organisation does present risks to efficiency and effectiveness. Although there is high visibility of information assurance and information technology at Board level, not all aspects of information and knowledge management are similarly covered at that level.

45. The Assessment Team found evidence of the effective management of information security and information risk. However, the risks of not sharing or exploiting information, or of failure to capture key information, were not always understood, or well managed by those interviewed. The Government's Managing Information Risk'[1] report provides guidance on identifying and managing risks within the public sector. This report was published as guidance for boards to sit alongside the Cabinet Office Data Handling Procedures which put in place Mandatory Minimum Measures to protect information.[2] Once the risks have been identified, this should guide the focus of FCO's KIM activity.

Recommendation 1: FCO Board needs to communicate to all staff that they are committed to improving information management, including having a Board champion for knowledge and information management.

---

[1] Managing Information Risk

[2] Mandatory Minimum Measures

Recommendation 2: FCO needs to raise understanding and accountability for information management, through the establishment of a high level body that has responsibility for the strategic direction and governance for KIM.

Recommendation 3: FCO should consider setting up an information change management programme as a key part of I&TD's ICT strategy to raise awareness of information management and drive information-related change, including the better understanding of not sharing or exploiting information, or failing to capture information.

Information Management Officers (IMO)

46. As part of the roll out of Firecrest 3rd Generation (F3G), FCO have created a number of roles called Information Management Officers (IMO) and Information Support Officers (ISO). These roles are a bolt on to the substantive role of generalist staff, with the expectation that it should take up no more than 5-10% of the staff member's time. The IMO resource has focused, to date, on data preparation and the management of tasks needed in advance of the rollout of F3G; there was little evidence that the IMO role is being used to raise the understanding of information management within FCO. The Assessment Team believe that FCO should maximise the potential of the IMO and ISO roles in supporting the wider information management agenda.

47. As administrators of the i-Records system, the IMOs could use knowledge of file plan to support departmental KIM. However, the IMOs as yet do not have a formal network to share experiences, knowledge and best practice. As this role is key to enabling the success of the Firecrest infrastructure, it would be beneficial to ensure that there is a forum for the IMOs and ISOs, otherwise there is a risk that FCO is not making use of user experiences in both operating and managing the system. The IMO network could also be a conduit to feed changes and raise standards of information management across FCO.

48. The overall responsibility for the IMO role in the UK was due to be

handed over from Business Engagement Group to IMG at the end of March 2010. Additionally, approximately a quarter of IMOs at posts overseas have also been handed over to the IMG. This is to be commended.

Recommendation 4: FCO should consider developing the IMO role to give them an active role in supporting the KIM strategy and raising the profile of effective records and information management practice within the Department.

Risk Management

49. FCO has an established risk management policy and corporate risk management procedures in place that are well understood. The need to control high classification material is understood and put into practice across the organisation. There is a very strong culture of protection for high classification documents. Checks are in place across the board to ensure correct handling of high classification papers, for instance the electronic tracking of papers between buildings, including their destruction.

Records Management

"I will ensure that our information is appropriately captured, described, managed and preserved and that the risks are controlled." [Peter Ricketts]

What to Keep

50. FCO needs to define what corporate information needs to be kept. This should be regardless of the format of the information. For instance, there may be important content held within an email or on a blog, and while FCO does have guidance in this area, it needs to ensure that this is applied in practice. The Assessment Team found there was a widely held perception in the FCO that only information that "was for the public record" should be kept. When questioned on what constituted "for the public record" many of those interviewed stated that it was information which they thought would eventually be sent to The National Archives. FCO should not be keeping information solely because it believes it will be of subsequent historic interest: information that has current legal and evidential value should be kept, and it should be adequately protected through records management controls (rather than just kept on shared drives). There is a risk that although there may be a "general" understanding of what should be for the public record, without a clear steer this is open to numerous interpretations and poses a risk that information perceived as "not having value" will not be kept as part of FCO's legacy.

51. The decision on what information is to be kept has to be made at a corporate and senior level in the Department. Once this has been decided it must then be communicated to all FCO staff via appropriate procedures and guidance, because there is a real risk that corporate information that is important to FCO will not be saved - as the value or the relevance of the information may not be recognised.

Recommendation 5: FCO should define what corporate information needs to be kept across all its systems and areas at a senior and corporate level, and ensure that this is understood and disseminated.

52. There was concern expressed by some Managers that with the move to more digital and collaborative working practices, FCO runs the risk of being unable to effectively find information. This is perceived to be caused by a number of contributing factors such as corporate administrative changes, introduction of new systems, the unforeseen growth in the use of email, and the potential plethora of storage areas with the introduction of SharePoint, and the lack of an enterprise search capability.

Recommendation 6: FCO should address the lack of an enterprise search capability.

Digital Continuity

53. FCO are a core funder of the National Archives' Digital Continuity project, sit on the project governance board, and have made a substantial contribution to shaping the continuity service for government. FCO is to be commended for being the first government Department to have drawn up a specific digital continuity strategy. The strategy identifies a whole-lifecycle approach to digital information management as being a key enabler for continuity. The work leading up to the strategy describes the organisational, technical and systems landscape to enable judgments about where the biggest continuity risks lie. The strategy identifies the risk of loss of continuity in the current technical environment as low, but the risk of loss of continuity in respect of specific older information, such as the information held on the Minerva system is high.

54. However, there is little evidence yet of high-level visible support for ensuring digital continuity within FCO. Understandably, the F3G roll-out has so far been the priority. Going forward, it will be important that the FCO digital continuity strategy is given senior management support and appropriate resourcing to ensure that digital continuity risks are appropriately mitigated.

Recommendation 7: CIO to agree with IMG how the digital continuity strategy within FCO will be resourced and prioritised.

55. The strategy identifies a more intractable, deep seated and dispersed problem: the increasing continuity risk over time because of the poor

management of digital information across the business.

Recommendation 8: Because of the crossover with general information management requirements, the digital continuity strategy should be embedded in the KIM strategy to facilitate a simpler structure for action and to maximise senior management support.

56. The relationship between information management (IM) and information technology is at the core of successful continuity and successful delivery of IT projects; IMG should seek co-sponsorship of the strategy from colleagues in other teams within I&TD, and should work with them to identify which collaborative information management and IT actions should be undertaken to ensure delivery of the digital continuity strategy. This should include: embedding continuity requirements in the IT change management processes, determining a way forward for Minerva and developing other archiving solutions e.g. for moving information out of i-Records into an archive; working to embed IM requirements in the enterprise architecture going forward; identifying specific file format obsolescence issues which need addressing; developing the IM aspects of enterprise search and content analysis requirements, so that information assets can be appropriately mapped and evaluated, and the future problem of sensitivity review can be properly addressed.

Recommendation 9: IMG should form a closer working relationship with colleagues in other teams within I&TD, and specifically with the IT Security Advisers, to ensure that digital continuity is properly embedded in the Information Asset Register process.

Recommendation 10: FCO to develop archiving solutions, and information management aspects of enterprise search to enable future electronic sensitivity reviews.

57. In line with the development of the HMG Information Assurance Maturity Model and Assessment Framework's (IAMM's) Information Asset Register (IAR) definition by Cabinet Office and The National Archives, the FCO IAR should be developed further as a vehicle to describe the information assets themselves (rather than just the

systems they sit on) and their ongoing usefulness to the business. This will help define the digital continuity requirement. Information asset owners should be held accountable for ensuring the digital continuity requirements of their assets, as described in the IAR, and that these are being addressed in line with the requirements of the IAMM. The IMO network should be used to support this process.

Recommendation 11: The IAR should be developed to describe the information assets and the accountability for continuity requirements.

Recommendation 12: Against the background of highly constrained resources, IMG should work with The National Archives to identify which digital continuity interventions should be prioritised on the basis of impact and ease of implementation.

Recommendation 13: IMG should work with The National Archives to identify how the developing digital continuity guidance and framework of tools and services might be exploited by FCO to implement their digital continuity strategy.

Recommendation 14: IMG should ensure that the IMO network is used to support the IAR process.

Legacy Systems

58. FCO has a legacy system called MINERVA (that predates Firecrest Registry and i-Records) which holds records going back more than 15 years. The MINERVA database is located within the Records Management Team in Hanslope Park. While there were still some old records to be added to MINERVA, these are now held on a separate standalone computer because the MINERVA database does not have the capacity to ingest them. Staff are confident that the records that MINERVA does hold are well managed, although the search facility is limited.

59. The MINERVA database is currently maintained by an external contractor, and FCO has been advised that the contractor cannot

guarantee that the specialist skills and knowledge required will be available beyond March 2011. FCO is aware of this and is currently looking at solutions to remedy the situation.

60. Despite the knowledge that access to the records held on MINERVA needs to be ongoing, this risk has not had sufficient profile in the FCO.

Recommendation 15: FCO should mitigate the risk that the records held on MINERVA become inaccessible in the long term by raising awareness of the risk and developing a transition plan.

Private Offices

61. The impact of the FCO Private Offices' function is quite far-reaching in an international government Department such as FCO. The Private Offices are well run with clear and effective processes and procedures, however, there was no written guidance on information management and staff within Private Offices relied on personal knowledge transfer. This should be a priority for the FCO to address in order to effect a smooth transition in the event of any ministerial or senior changes.

62. Private Offices in FCO follow Model Two from the Cabinet Office[3] 'Guidance on Private Offices'. This is acknowledged within the Guidance as the model that poses the most risk to a Department. In a Department that is not mature in how it manages its information across the board, there is potentially a serious risk as the management of Private Offices information is devolved to a large number of teams and individuals.

63. This system relies upon the Private Offices being assured that policy units are keeping a full and accurate record of all correspondence. As FCO is yet to determine what information should be kept corporately, there is significant potential for major reputational damage if records are not available to justify the decision making process.

Recommendation 16: FCO should develop written guidance on information management for Private Office staff.

[3] Guidance for Private Offices

Recommendation 17: FCO should undertake an annual assessment of Private Office procedures to fully comply with Cabinet Office and National Archives guidance.

i-Records (electronic document and records management system)

64. i-Records is not being used as effectively as it should be within the FCO. Although the registration on i-Records is an improvement on the previous system (Firecrest Registry), it is still not at the right level of quantity or quality. There is a general level of frustration amongst staff with i-Records, particularly with their ability to search and retrieve records. It is often easier for staff in some teams to use other external sources and the IT systems of other organisations to find information. The use of Metadata is a critical issue for FCO, which needs to train staff on the importance of metadata.

65. Likewise staff also find it difficult to retrieve documents by subject, and therefore the FCO needs to make it easier to retrieve information, and needs to develop a controlled vocabulary to aid the search experience.

66. There is currently also an inability to lock down permissions on folders in i-Records, which limits the type of material which can be registered or declared as records. This is a high priority for FCO and is currently in development. This is especially important when access to such information is given to those overseas locally engaged (LE) staff who have not previously had the ability to use the FCO's electronic records management systems. Adequate training and guidance for LE staff should be provided with appropriate permissioning applied to folders on i-Records. The FCO has only recently started to use statistics to check the rate of registration. Staff have a choice of where to store and keep their information which has led to fragmentation. Staff will often save information on shared or personal drives in preference to using i-Records. The risk, therefore, is that key information of business importance to the FCO is not kept appropriately, and so may not be accessible to the FCO when required.

Recommendation 18: FCO should ensure that i-Records has the ability to lock down the permissions on folders, and needs to develop a controlled vocabulary to aid searching.

Recommendation 19: FCO should make registry on i-Records for corporate information compulsory and check on appropriate usage as part of its regular KIM audits.

Recommendation 20: FCO should investigate how it can make i-Records more useable, particularly in relation to the search facility, and should ensure that i-Records can function in the long term as a proper managed records environment.

Shared Drives

67. The digital directory structures (shared areas) are organised in line with team structures. This can limit the opportunities for cross-working, which could improve the effectiveness of decision making and policy. There is no sense of shared systems - the FCO systems do not facilitate sharing and collaborative working.

68. Shared areas are often seen as an alternative to registry. Files are often stored on the shared drive rather than in i-Records, which is the official registry. There is a risk that important corporate information will not be findable, and that FOI requests will be more challenging to answer as the information is on several shared drives rather than in a central area and there is also a risk of duplication or omission. Although records are captured, information is not always managed as a key corporate asset.

69. The situation is exacerbated by the fact that large personal areas have been allowed under the new IT system Firecrest). Important corporate information is often stored in these personal areas rather than on i-Records or even shared areas.

Recommendation 21: FCO should give clear direction and guidance on the structure and appropriate usage of shared areas, and use audit to ensure that this guidance is followed. This should also be applied to any future systems that are introduced, such as Sharepoint.

Email

70. FCO has an email management policy, but the majority of interviewees were not aware of the content of either the policy or how it affected their role. Any emails containing important corporate information should be stored on i-Records. There are a number of staff who were proactive in managing their emails and generally filed important information, as well as actively trying to keep the size of their inboxes within a manageable limit. In contrast, there were many examples of unsatisfactory practice where staff did not save information. If there is no check on the adherence to email policy, there is a potential for important corporate information to be lost.

Recommendation 22: FCO should reinforce compliance with the email policy.

Information Legality

"I will promote access to and re-use of our information, and protect personal and other sensitive information." [Peter Ricketts]

Freedom of Information (FOI)

71. The FCO has processes in place which enable it to meet FOI requests within statutory timescales. However, the Assessment Team has concerns about the completeness of some of the FOI responses. Records held in Minerva (where old Aramis files were stored when Firecrest originally came out) have caused issues in being able to locate and retrieve records. The search function on Minerva was restricted to a handful of staff and unreliable, with some Aramis records still waiting to be loaded onto Minerva from tape. Furthermore, there is anecdotal evidence that key corporate records have not been retained because they were only kept on personal drives and destroyed when the incumbent moved on.

72. Concerns were raised that there has been a decline in the registration of documents which is making information difficult to find. Often, Case Managers were not confident that all required information was found; they were reliant on desk officers to provide the information. FOI Case Managers only have access to information stored on corporate systems. They do not have access to information stored on local systems, paper systems in registries or local practices. Furthermore, there is no quality assurance on information provided in response to an FOI request. Case Managers complete the FOI eLearning package and course, but it is has not been mandatory for sensitivity reviewers to undertake similar training.

73. There were examples of good practice in relation to FOI. For example, FOI workshops and meetings were held and Case Managers provided induction training for newcomers to the Department.

Recommendation 23: FCO should introduce quality assurance procedures to ensure that FOI requests are complete and accurate.

Recommendation 24: FCO should implement mandatory FOI training for sensitivity reviewers.

Data Protection

74. The FCO has adequate processes in place for deleting high classification records. However, it needs better evidence that other records are actually being deleted. There are risks, for instance in not being able to find records or keeping personal information longer than required. However the migration of data from second generation Firecrest (F2G) to third generation Firecrest (F3G) has meant that large quantities of material has been sifted and deleted, and is a practice which should be maintained on an ongoing basis.

Recommendation 25: FCO to ensure that staff regularly delete personal data that is no longer required, in accordance with data protection principles.

Re-Use

75. FCO information is made available for re-use via the PSI Click-Use Licence operated by The National Archives. FCO enjoys a good working relationship with The National Archives in this area. FCO is keen to enable the re-use of its material and thus most of its material has historically been made available for re-use, first under the Core Click-Use Licence and more recently the PSI Licence.

76. The FCO has also provided dedicated support from within IMG to provide datasets for inclusion on the UK website data.gov.uk and is to be commended in this regard.

Data Security

77. Within certain parts of FCO, examples of good practice in data security were found. For instance, IMG has taken on board the Cabinet Office Data Handling Review Report, June 2008 and management of personal data. Data handling training is also mandatory for all contractors and consultants. However, concerns were expressed that this training was not necessarily carried out.

78. The two-tier marking of classified material poses the risk that different classifications of papers will be grouped together in files for expediency sake.[4] In order to keep the information all together, there is the temptation for staff to put all the information relating to a single topic either in the lower tier or in the confidential tier to avoid the problem of split information. This could lead to people having access in the lower tier to information they should not see. Conversely, they could have no access at all if the information is saved in the confidential tier.

Recommendation 26: FCO to ensure that data security training[5] is undertaken by all staff employed by FCO, regardless of the type of contract.

Recommendation 27: FCO should raise awareness of the need to correctly classify material and ensure that staff follow the guidance.

Parliamentary Questions (PQs)

79. In answering PQs, FCO staff often find it difficult to search historical information due to the search facility within i-Records. Instead, they tend to use the Internet to look for responses to similar questions in the past. There is a risk that answers may not be complete or consistent.

Sensitivity reviewing

80. Sensitivity review is the process by which FCO records are reviewed at the point of potential transfer to The National Archives in order to determine whether the records should be transferred open or closed, or redacted. Sensitivity reviewing at present only takes place on paper records held at Hanslope Park. There is no quality assurance of the reviews, instead relying on the experience and judgment of the

[4] File: the collection of information which might otherwise all exist in a single area in the file plan, as it would have done on a paper file.

[5] Cabinet Office's Protecting Information eLearning.

reviewers, although the application of all FOI and PRA exemptions is quality reviewed by other IMG staff.

81. The FCO should continue to seek ways to mitigate risks associated with this process, such as the correct application of FOI exemptions. There is a risk that the reviewers will base their decision on a subjective assessment. These reviewers, who are retired senior FCO staff are experienced, but have no formal training in the application of FOI exemptions. The Lord Chancellor's Advisory Council, which reviews all FCO recommendations for closures and redactions, has expressed concerns in recent years about the degree of variability of the FCO's justifications, and the lack of consistency in approach. FCO has a pool of sensitivity reviewers producing applications which invariably can lead to inconsistency in approach. These should be subject to a consistency check prior to being forwarded to The National Archives. FCO has not yet put arrangements in place to deal with the sensitivity reviews of electronic records.

Recommendation 28: FCO should address the training requirements of sensitivity reviewers.

Recommendation 29: FCO needs to consider its approach to sensitivity reviewing digital records, as these are likely to require a different approach to paper records. With the likelihood of a reduction of the 30 year rule to a 20 year transfer point, there will be a need to implement reviews of digital records in the near future.

Compliance

"I will make sure that our internal processes support effective information management." [Peter Ricketts]

Policies and guidance

82. Information management guidance is available on FCONet. The drafting of the guidance tends to be reactive, and drafted on request. The available guidance is adequate, but there are areas that should be covered, such as a need for more guidance for locally engaged staff, for example on classification guidance should also be relevant to staff working in particular operational areas such as visas. The Assessment Team has been advised that the Consular Directorate have developed its own data protection policy. Where there is no clear guidance, for example with the retention of Ministerial correspondence, staff have introduced their own practices leading to a lack of consistency and possible breaches of legal requirements. FCO need to ensure that they have oversight of all such polices to ensure that they fully comply with FCO policy.

Recommendation 30: FCO should review the completeness and relevancy of its existing Information Management Guidance to ensure it meets business needs.

Intranet

83. FCO's intranet, FCONet, contains a mass of information that is often very dense and not easily searchable. Individual teams are responsible for their own areas of FCONet and there is no consistency of approach in what is published. Valuable information, such as the Permanent Secretary's blog, is also published on FCONet but not kept anywhere else. There is a general perception that FCONet contains only current information and therefore has no relevance to records management. It is, however, a valuable tool for disseminating good practice and should be used as such.

Recommendation 31: FCO to review the content and policy of its Intranet site to ensure that is easily searchable, up to date and that corporate records are registered.

Training

84. As with many other Departments, FCO has provided roll-out training to support the launch of new systems. However, this is not provided on an ongoing basis and the training is also now optional. By making training optional, FCO loses its capacity to change behaviour and to instil good practice. Additionally, the training for i-Records was often provided well in advance of local file plans being set up and ready to use, which meant that many staff had forgotten what they had learnt by the time they were able to use the system.

85. The FCO's induction training does not cover information management. Some induction training within FCO covers FOI, data handling and DPA, but does not contain any training on more general records or information management. IMG has identified information management training needs, for instance on FOI.

Recommendation 32: IMG's KIM training needs analysis should be implemented.

Recommendation 33: All FCO induction training should include a session on KIM.

Information Audit

86. The FCO carries out information audits of paper and electronic records on i-Records, which is to be commended. However, these audits have limited scope, for instance not covering wider information management practice. They also lack a sufficiently prominent profile and are given a low priority within the Department. There is also currently no formal process for the sharing of good practice or lessons learned from these audits.

Recommendation 34: FCO should give consideration to expanding the scope and remit of the information audits, developing them on a Financial Audit model.

Recommendation 35: FCO should share good practice and lessons learned from the information audits.

Culture

"Information is recognised as a key asset for running the business of the Foreign and Commonwealth Office and is used to support effective data and information sharing and knowledge creation." [Peter Ricketts]

87. The FCO's role is to run a global network for the whole of the British government; deliver services to British citizens and pursue the government's foreign policy priorities. The FCO has a programme of change, which aims to make the organisation better at doing this in the world of the 21st century. Part of the change involves embracing different ways of thinking and working by encouraging new ideas, innovation and knowledge sharing, while reducing bureaucracy and process. Senior leadership believe there is more to do to take advantage of accumulated experience and knowledge, establish continuity and avoid "reinventing the wheel"; there is a great appetite to exploit the new tools and techniques more effectively. FCO understands the need to balance the flexibilities and freedoms from improved knowledge sharing with information management policies and processes that align with best practice. However, it is imperative that the FCO sets its own high standards and the mechanisms to audit and review how systems and processes work. Without this there is likely to be little corporate accountability and staff will continue to work as individuals.

88. The IMO network will be an ideal vehicle through which to share best practice and disseminate new ways of working across FCO. Staff recognise that sharing information is more than just a change in how systems are used. FCO has to create a culture that is open to sharing information and not one that shares on a "need to know" basis. Even information that can be anonymised for wider internal dissemination is not shared readily. The KIM Strategy and IMO network need to address this.

89. Many of those interviewed by the Assessment Team did not fully understand the value of the historical or corporate information that they held and created, excepting where information is needed for immediate use. The culture of information sharing is not mature or embedded across the FCO and many staff do not understand how the information they use, possess and process could benefit the FCO other than for its immediate purpose. The majority of the information tends to be held within business areas and not shared. The Assessment Team found examples of staff who would look for FCO information via external search engines as it was easier than trying to find the information held on systems within the Department.

90. There are pockets of good practice across the FCO which are to be commended. The FCO is one of the few Departments that has an in-house 'official histories' team. Similarly the Research Analysts have very clear drivers for high integrity information storage, discovery and re-use, for instance the frequent need to consult historical data or information in order to produce and justify a piece of analysis. This is reflected in how their performance is measured, which has driven a strong local culture amongst Research Analysts of records and knowledge management. FCO could explore whether they can replicate the clarity and importance of information management drivers across the rest of the organisation. Staff should be encouraged to value and make better use of its own, valuable information.

91. IMG needs to be at the heart of IT projects and IT system upgrades, because their lack of involvement in some areas of the organisation has had a negative impact on the ability of the FCO to drive up information standards and assure consistent information management handling across IT systems. FCO also needs to recognise that effective information management is the business and responsibility of all staff in FCO, not just the few in specialist roles. Raising the profile of knowledge and information management has to be part of an organisation wide cultural change programme that encompasses

systems, training and on-going support. Treating each part as separate components increases the risk of failure of some or all parts of the programme, leading to a loss of credibility, both internal and external, to the Department.

Recommendation 36: FCO should effectively raise the profile of information management across the Department, and ensure that IMG is at the heart of the development of new IT systems, their training programmes and on-going support.

92. The delivery of the i-Records system has been the primary focus as part of wide programme of IT system upgrades across the Department. To realise the full potential of the investment and to ensure that the i-Records system is used effectively, FCO needs to make sure that information management is clearly linked into ongoing training and support for i-Records. A joined-up approach will also aid the overall change in behaviour regarding managing information that FCO should be seeking. This will ensure that staff are clear how the i-Records system is to be used and reinforce the fact that it should be the main location of documentation storage.

93. A challenge for FCO is to get the balance right between mandating through guidance and implicit instructions, and allowing areas to make their own decisions. FCO has out of necessity, operated with an expected amount of autonomy for daily decision making and use of low level systems. The information landscape has changed and FCO needs to continue to be flexible, but with clear parameters so that daily business continues and core information is captured. With all systems there are exceptions. FCO needs to be sure in what areas of the business non-core systems are used, and who has the ultimate responsibility for them. If not, there is a risk that the confusion about what systems are mandatory or not will continue, and open FCO up to potential legal challenge if information cannot be located.

Recommendation 37: FCO needs to ensure that staff are clear how the i-Records system is to be used and that it should be the main storage location of all documentation.

Knowledge Transfer

94. FCO staff generally change roles on average every 2-3 years and this can lead to not only a loss of knowledge, but a disruption in working practices as staff move from one job to another. FCO is perhaps not making the best use of the knowledge that its staff have gained through either working overseas or within the United Kingdom. For instance, personal knowledge from staff leaving the organisation or transferring back to the UK from overseas offices is not routinely captured.

Recommendation 38: FCO to establish formal handover procedures to capture knowledge on internal transfer.

APPENDIX ONE: SUMMARY OF RECOMMENDED ACTIONS

This is a summary of the recommended action to:

- remedy the weakness identified; and,
- strengthen the commitment to the Information Management Assessment Programme.

These recommendations, when implemented, will provide significant benefits to the organisation. Most notably, these will include:

- Providing business continuity and consistency;
- Protecting access and retrieval of vital information;
- Providing evidence of decision making;
- Being accountable and transparent;
- Providing an audit trail of actions;
- Being compliant with current legislation;
- Minimising risk of loss of vital information and security breaches;
- Increasing effectiveness and efficiency; and,
- Reducing overall corporate costs.

These actions will form an Action Plan that will be monitored.

Business Area	Ref	Recommendation
Governance	1	FCO Board needs to communicate to all staff that they are committed to improving information management, including having a Board champion for knowledge and information management.
	2	FCO needs to raise understanding and accountability for information management, through the establishment of a high level body that has responsibility for the strategic direction and governance for KIM.
	3	FCO should consider setting up an information change management programme as a key part of I&TD's ICT strategy to raise awareness of information management and drive information-related change, including the better understanding of not sharing or exploiting information, or failing to capture information.

	4	The FCO should consider developing the IMO role to give them an active role in supporting the KIM strategy and raising the profile of effective records and information management practice within the Department.
Records Management	5	FCO should define what corporate information needs to be kept across all its systems and areas at a senior and corporate level, and ensure that this is understood and disseminated.
	6	FCO should address the lack of an enterprise search capability.
	7	CIO to agree with IMG how the digital continuity strategy within FCO will be resourced and prioritised.
	8	Because of the crossover with general information management requirements, the digital continuity strategy should be embedded in the KIM strategy to facilitate a simpler structure for action and to maximise senior management support.
	9	IMG should form a closer working relationship with colleagues in other teams within I&TD, and specifically with the IT Security Advisers, to ensure that digital continuity is properly embedded in the Information Asset Register process.
	10	FCO to develop archiving solutions, and information management aspects of enterprise search to enable future electronic sensitivity reviews.
	11	The IAR should be developed to describe the information assets and the accountability for continuity requirements.
	12	Against the background of highly constrained resources, IMG should work with The National Archives to identify which digital continuity interventions should be prioritised on the basis of impact and ease of implementation.
	13	IMG should work with The National Archives to identify how the developing digital continuity guidance and framework of tools and services might be exploited by FCO to implement their digital continuity strategy.
	14	IMG should ensure that the IMO network is used to support the IAR process.
	15	FCO should mitigate the risk that the records held on MINERVA become inaccessible in the long term by raising awareness of the risk and developing a transition plan.

	16	FCO should develop written guidance on information management for Private Office staff.
	17	FCO should undertake an annual assessment of Private Office procedures to fully comply with Cabinet Office and National Archives guidance.
	18	FCO should ensure that i-Records has the ability to lock down the permissions on folders, and needs to develop a controlled vocabulary to aid searching.
	19	FCO should make registry on i-Records for corporate information compulsory and check on appropriate usage as part of its regular KIM audits.
	20	FCO should investigate how it can make i-Records more useable, particularly in relation to the search facility, and should ensure that i-Records can function in the long term as a proper managed records environment.
	21	FCO should give clear direction and guidance on the structure and appropriate usage of shared areas, and use audit to ensure that this guidance is followed. This should also be applied to any future systems that are introduced, such as Sharepoint.
	22	FCO should reinforce compliance with the email policy.
Information Legality	23	FCO should introduce quality assurance procedures to ensure that FOI requests are complete and accurate.
	24	The FCO should implement mandatory FOI training for sensitivity reviewers.
	25	FCO to ensure that staff regularly delete personal data that is no longer required, in accordance with data protection principles.
	26	FCO to ensure that data security training is undertaken by all staff employed by FCO, regardless of the type of contract.
	27	FCO should raise awareness of the need to correctly classify material and ensure that staff follow the guidance.
	28	FCO should address the training requirements of sensitivity reviewers.

	29	FCO needs to consider its approach to sensitivity reviewing digital records, as these are likely to require a different approach to paper records. With the likelihood of a reduction of the 30 year rule to a 20 year transfer point, there will be a need to implement reviews of digital records in the near future.
Compliance	30	FCO should review the completeness and relevancy of its existing Information Management Guidance to ensure it meets business needs.
	31	FCO to review the content and policy of its Intranet site to ensure that is easily searchable, up to date and that corporate records are registered.
	32	IMG's KIM training needs analysis should be implemented.
	33	All FCO induction training should include a session on KIM.
	34	FCO should give consideration to expanding the scope and remit of the information audits, developing them on a Financial Audit model
	35	FCO should share good practice and lessons learned from the information audits.
Culture	36	FCO should effectively raise the profile of information management across the Department, and ensure that IMG is at the heart of the development of new IT systems, their training programmes and on-going support.
	37	FCO needs to ensure that staff are clear how the i-Records system is to be used and that it should be the main storage location of all documentation.
	38	FCO to establish formal handover procedures to capture knowledge on internal transfer.

APPENDIX TWO: IMA COMMITMENT

I am personally committed to making sure that we create and manage the information we need to fulfil our corporate obligations. To show the strength of my commitment, both in FCO and to our partners, I have asked The National Archives to begin the process of assessment. The National Archives final report will be published.

I will provide effective leadership on Knowledge and Information Management capability across my Department. I will make sure that our internal processes and training support effective information management. Information is recognised as a key asset in FCO and is used to support effective data and information sharing and knowledge creation. I will ensure that our information is appropriately captured, described, managed and preserved and that the risks are controlled. I will promote access to and re-use of our information, and protect personal and other sensitive information.

Peter Ricketts

Permanent Secretary

APPENDIX THREE: GLOSSARY

CIO	Chief Information Officer
DPA	Data Protection Act
F2G	Second-generation Firecrest
F3G	Third-generation Firecrest
FCO	Foreign and Commonwealth Office
FOI	Freedom of Information
I&TD	Information and Technology Directorate
IAMM	Information Maturity Model and Assessment Framework
IAO	Information Asset Owner
IAR	Information Asset Register
ICT	Information and Communication Technologies
IM	Information management
IMA	Information Management Assessment
IMG	Information Management Group
IMO	Information Management Officer
ISO	Information Support Officer
LE	Locally Engaged
KIM	Knowledge and Information Management
OGLO	Open Government Liaison Officer
PQ	Parliamentary Question
PRA	Public Records Act
PSI	Public Sector Information