The National Archives

# Information Management Assessment

## Department for Culture, Media and Sport

### April 2012

**Agreed in December 2010 to allow time for DCMS to prepare a statement of progress**

Contents

## PART ONE: EXECUTIVE SUMMARY

1.1 There is recognition that the Department for Culture, Media and Sport (DCMS) must change how it manages its information. The 2009 Cabinet Office information risk return provided evidence of how its information assurance management and responsibilities were not effective. Since then, the need to improve knowledge and information management has been recognised, as evidenced by the steps being taken to address issues stemming from DCMS' data handling review. Senior management acknowledge that they need assurance that DCMS can meet other statutory obligations such as The Public Records Act 1958, Data Protection Act 1998, and Freedom of Information Act 2000. This Information Management Assessment (IMA) is an active first step in understanding the key risks.

1.2 A positive start has been made in identifying the key departmental information assets. The information asset register covers core DCMS and the Government Olympic Executive. DCMS has provided a definition of business critical information, but the value of this information has not been fully defined. Work has started on applying consistency to this. DCMS does not know fully what information it needs to keep. Without this knowledge, DCMS will not be able to manage, exploit or safeguard its information. Although many good local practices are in place, there is no corporate assurance that local policies and practices are working. DCMS should continue its steps to comprehensively address what information is business critical. Until this is done there will continue to be a substantial risk to the corporate memory of DCMS, and also the risk that DCMS will not be able to find, protect or use its information.

1.3 DCMS has yet to fully identify the risks associated with managing and safeguarding the information it holds and creates. Often, senior management and staff only consider personal information to be within the remit of information assurance, with little overt value being placed on corporate business information and other categories of sensitive information. Notification of information risks at senior management level is via the Audit Committee. There was no evidence that information risk was being fully identified and acted upon at a lower level.

1.4 The assessment team found no evidence that information management issues were being regularly reported to the Board. Such reporting would indicate that DCMS was ready and able to consider information management at a strategic level. Without senior level understanding and commitment to information management there is a real risk that key information will be mismanaged. DCMS needs to demonstrate senior management engagement and commitment to information management as this is vital to raise DCMS' capability. DCMS is exposed to serious reputational risks if information relating to key business and policy decisions is lost, cannot be found or cannot be proved to be authentic. A board member with corporate responsibility for knowledge and information management (KIM) is required to give the strategic direction and understanding on information management (IM) and information assurance (IA) for managers and staff.

1.5 Without a defined structure for knowledge and information management, DCMS is limiting its potential to exploit and make full use of its information assets. The assessment highlighted several areas across DCMS where key roles and responsibilities relating to IA and IM were not fully developed, assigned or were absent. For example, DCMS did not have a substantive departmental records officer (DRO), while the temporary head of information management and assurance was on a fixed-term contract at the time of assessment. Unless such roles are resourced, DCMS is at risk of being non-compliant in its legal obligations for records management.

1.6 LiveLink is DCMS' primary system for the storing of electronic documents and records. Specialist 'information champion' support roles were created to support its implementation. Negative perceptions have since emerged concerning use of LiveLink due to the difficulty in searching and retrieving information. Some staff often avoid using the system and use desktops, personal or shared drives to store information. The risk that this behaviour poses to DCMS is that it will not have a definitive version of a document or record, and therefore DCMS will be unable to support informed decision-making and be in breach of its public record responsibilities.

1.7 LiveLink has limited guidance on naming conventions which has created a problem with browsing within the system. For example, it is often difficult

to find information outside particular work areas. This impacts on the ability to understand the context of information and time spent trying to retrieve information.

1.8 Although staff interviewed stated information on LiveLink could be 'ring-fenced', there was evidence that this was inconsistent. Staff did not always distinguish between personal and sensitive information, including material such as negotiations on Football Association contracts, where a breach of confidentiality would carry a risk of reputational harm to the Department. DCMS has a duty to protect the information it holds and to ensure that these responsibilities are communicated. DCMS should ensure a continuous programme of training and maintain a core of 'expert' users across the department to facilitate effective use of LiveLink.

1.9 The assessment team was aware that many of those interviewed appeared to view DCMS as a series of co-located business areas, rather than a single department with a central set of goals. This has contributed to the development of individual working practices, rather than unified compliance with corporate policies and practices. This makes it difficult to either mitigate information risks or to exploit information resources.

1.10 DCMS has provided a corporate steer on answering Parliamentary Questions and Freedom of Information requests. This priority and clarity of message should be extended to other aspects of knowledge and information management.

1.11 Good information management is the foundation of good information assurance. By addressing the recommendations contained in this report, DCMS will be taking the required steps to achieve its commitment towards a structured strategic approach to knowledge and information management. This will provide DCMS with assurance that it is meeting its statutory obligations. DCMS should make full use of the advice, support and guidance provided by The National Archives, Government Knowledge and Information Management Network and other bodies such as Cabinet Office to achieve this.

**Risk Matrix**

1.12 The risk matrix result is a culmination of the pre-assessment analysis, onsite interviews, and evidence submitted.

**Governance and leadership**

| | | |
|---|---|---|
| Strategic management |  | Priority Attention Area |
| Business objectives |  | Priority Attention Area |
| Management controls |  | Priority Attention Area |
| Resourcing |  | Priority Attention Area |
| Risk management |  | Development Area |

**Records management**

| | | |
|---|---|---|
| Creation |  | Satisfactory |
| Storage |  | Development Area |
| Appraisal, disposal and transfer |  | Development Area |
| Sustainability of digital records |  | Development Area |
| Management |  | Priority Attention Area |

**Access to information**

| | | |
|---|---|---|
| FOI/Data Protection |  | Development Area |
| Re-Use |  | Good |
| Security |  | Priority Attention Area |

**Compliance**

| | | |
|---|---|---|
| Staff responsibilities and delegations |  | Development Area |
| Policies and guidance |  | Satisfactory |
| Training |  | Development Area |
| Change management |  | Satisfactory |

**Culture**

| | | |
|---|---|---|
| Commitment |  | Development Area |
| Staff understanding |  | Satisfactory |
| Knowledge management |  | Development Area |

| Key to colour coding | |
|---|---|
| | **Best Practice** |
| | **Good** |
| | **Satisfactory** |
| | **Development Needed** |
| | **Priority Attention Area** |

# PART TWO: INTRODUCTION

## Information Management Assessments

2.1 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, sustainability, 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
- helps accounting officers plan for future information management developments.

2.2 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 via robust, independent validation of the standards and integrity of the information management processes, and capability within departments.

2.3 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.

2.4 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.

2.5 This report sets out the findings, conclusions and recommendations of The National Archives' Information Management Assessment of the Department for Culture, Media and Sport (DCMS).

**The business of the Department for Culture, Media and Sport**

2.6 The department was created in 1992. In May 2005 DCMS expanded its brief to the creative industries, gaining responsibility for fashion design, advertising and the arts from the Department for Business, Innovation and Skills (BIS), formerly the Department for Business, Enterprise and Regulatory Reform (BERR).

2.7 DCMS was restructured in 2008 to support a more focused, flexible and influential way of working. In 2009 the department was organised into five directorates that are intended to work flexibly across boundaries to ensure corporate aims and objectives are delivered. Policy and programmes are delivered by the Government Olympic Executive and the Partnerships and Programmes directorate, while the corporate centre is formed of the External Relations and Corporate Services directorate. The Culture, Media and Sport Sector teams form the core of DCMS' policy areas.

2.8 The department's aim is:

> **'To improve the quality of life for all through cultural and sporting activities, support the pursuit of excellence, and champion the tourism, creative and leisure industries'.**

2.9 DCMS sets Government policy on the arts, sport, the National Lottery, tourism, libraries, museums and galleries, broadcasting, creative industries including film and the music industry, press freedom and regulation, licensing, gambling and the historic environment. DCMS is also responsible for the 2012 Olympic Games and Paralympic Games.

2.10 According to its 2009 annual report, DCMS has responsibility for a wide range of activities, from the listing of historic buildings and scheduling of ancient monuments, export licensing of cultural goods, to management of

the Government Art Collection and The Royal Parks. The department's ceremonial duties include co-ordinating aspects of state visits and the Annual Service of National Remembrance at the Cenotaph.

2.11 DCMS is also responsible for providing a co-ordinated approach to aftercare for the survivors and bereaved relatives of major disasters through the Humanitarian Assistance unit. In this capacity DCMS was responsible for managing the work to create the memorial in Hyde Park to victims of the 7/7 bombings.

2.12 DCMS works jointly with a number of other departments including the Department for Business, Innovation and Skills (BIS) on digital switchover, design issues (including sponsorship of the Design Council) and on relations with the computer games and publishing industries. The two departments together published the Digital Britain white paper on 16 June 2009. DCMS shares responsibility for policy on children's play with the Department for Children, Schools and Families (DCSF).[1]

2.13 DCMS has four departmental strategic objectives (DSOs) covering the period 2008-11. These are:

- **DSO1: Opportunity**: encourage more widespread enjoyment of culture, media and sport
- **DSO2: Excellence**: support talent and excellence in culture, media and sport
- **DSO3: Economic impact**: realise the economic benefits of the department's sectors
- **DSO4: Olympics and sport for young people**: deliver a successful and inspirational Olympic and Paralympic Games in 2012 that provide for a sustainable legacy and get more children and young people taking part in high-quality PE and sport.

2.14 DCMS works in what is described as 'a complex delivery environment', featuring an arms-length relationship (via funding, regulations and

[1] Now the Department for Education (DfE).

sponsorship) with the 56 sponsored bodies that help deliver the department's strategic aims and objectives. These include three public corporations, two public broadcasting authorities, one executive agency and 47 non-departmental public bodies (NDPBs). The latter range from Arts Council England and the UK Film Council to the Sir John Soane's Museum and the National Portrait Gallery.

## Information Management at the Department for Culture, Media and Sport

2.15 DCMS only has one full-time knowledge and information management role, which is the head of information management and assurance. There is also half of a post designated as a records manager.

# PART THREE: ACTIVITIES CARRIED OUT BY THE ASSESSMENT TEAM

**Methodology**

3.1 The underlying purpose of the assessment is to establish whether the key elements of DCMS' commitment to the IMA programme and its own knowledge and information management priorities are achieved.

3.2 Knowledge and information management is a set of processes which:

- collect, organise and maintain business information over time and make it readily accessible to the people who need it
- enable the collective and systematic creation, sharing and application of knowledge across an organisation.

The overall aim is to increase the efficiency and effectiveness of the organisation, the quality of its outputs, and its ability to effect change.

3.3 A range of standard processes, systems and documentation were examined to determine the effectiveness of KIM within the organisation. 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.

3.4 DCMS 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
- information management or skills issues raised by DCMS.

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; and data handling processes. |
| Records management | The creation, storage, appraisal, disposal, transfer, security, management and sustainability of digital and paper records |
| Access to information | Access to and re-use of government information; websites and equivalents and the Freedom of Information and Data Protection Acts |
| Compliance | Staff responsibilities and delegations; policies and guidance; the intranet; skills and training; and the 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; and knowledge management |

**Activities undertaken**

3.5 The assessment took place between 22 and 26 February 2010 at DCMS's head office in London. The assessment team examined key policy and practice documentation relating to training, skills and processes and interviewed staff members from across the organisation. These activities are described in more detail below.

**Documentation review**

3.6 DCMS provided documentation in support of its information management objectives and the IMA commitment, which was reviewed prior to the on site assessment.

### People and practices

3.7 The assessment team interviewed a range of staff at all levels, who are involved in policymaking, interpretation and the practice of managing information. These interviews were used to determine how people in the organisation work and the impact of information management on them.

### Process testing

3.8 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.

### Risk Assessment

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

### Data Handling

3.10 The department's data handling was reviewed in a limited context or 'light touch' within the IMA process and only where there is an immediate effect on the process being reviewed.

### The assessment team

3.11 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:

- head of standards
- information management consultants
- standards adviser
- head of information security and assurance
- a member of The National Archives' digital continuity team.

**Assistance provided by the Department for Culture, Media and Sport**

3.12 The National Archives wishes to thank all the staff in DCMS who took part in the assessment, especially the Head of Information Management and Assurance.

# PART FOUR: HIGHLIGHTS AND AREAS FOR IMPROVEMENT

## Governance and leadership

'I am personally committed to ensuring that we create and manage the information we need to fulfill our corporate obligations' Jonathon Stephens[2]

### Strategic direction

4.1 The executive board of DCMS has recognised the need for a change in the way it manages its information. The 2009 information risk return provided evidence that DCMS was not effectively managing its information assurance responsibilities. DCMS has since recognised the need for good knowledge and information management (KIM) within the department. Senior management also now acknowledge that they need assurance that DCMS can meet its other statutory obligations under the Public Records Act 1958, Data Protection Act 1998, and Freedom of Information Act 2000. This Information Management Assessment is an active first step in understanding what key risks need to be addressed.

4.2 At a local level, staff manage information well to do their jobs properly and the assessment team found many examples of good local information management practices within DCMS. For example, the Legal Team use the Treasury Solicitors' model for good information management. However, there is an absence of strategic direction and coordination on KIM across DCMS. The department did not have a KIM strategy at the time of the onsite assessment; therefore it has not been assessed. There was no regular performance reporting on information management. Regular reporting of information management would enable senior management to raise the visibility and assess the progress of information management across DCMS. Senior management has considered the information security agenda, as evidenced by the use of encrypted laptops and the existence of guidance on information security. This is a good first step and needs to be extended to other areas of information management.

4.3 Senior management engagement and a demonstrable commitment to KIM

[2] Permanent Under Secretary Statement of Commitment, 24 February 2010

are vital if DCMS is to raise its information management capability. DCMS may expose itself to serious reputational risks if information relating to key business and policy decisions is lost, cannot be found, cannot be proved to be authentic, has lost its context or cannot be transferred to another department as a result of machinery of government change. DCMS must raise awareness of knowledge and information management at the strategic level.

**Recommendation 1: DCMS should identify how to position information management strategically in DCMS and provide the appropriate support, resources and guidance at board level to achieve this**

4.4 The lack of strategic direction also impacts on how DCMS as a department is perceived internally. There was limited recognition of any consistent corporate message or 'branding' for DCMS as a whole. However, where the importance of a goal is understood and accepted DCMS is able to communicate this effectively and efficiently to staff. During the onsite assessment the team noted the emphasis placed on hitting the targets and time limits established for answering Parliamentary Questions (PQs), underlined by a poster campaign throughout the department. There is a clear steer on prioritising responses to PQs and DCMS has performed effectively in this regard. DCMS needs to apply this same level of priority and clarity of message to information management.

**Structure**

4.5 DCMS does not have an effective structure for managing KIM. The board should designate a board member with corporate responsibility for KIM. This will help champion KIM throughout the department and keep senior management abreast of progress across DCMS.

**Recommendation 2: The board should designate a senior champion to have corporate responsibility for KIM**

**Recommendation 3: The role with overall responsibility for KIM should lead on developing the long-term vision and plan for KIM for DCMS**

4.6 There is no senior responsible owner for digital continuity, nor any strategy

or action plan to manage digital continuity. DCMS needs to assign this responsibility at the same time that it assigns other senior level responsibilities that have been identified in this report. DCMS should refer to The National Archives' *Managing Digital Continuity* guidance to facilitate this.[3]

**Recommendation 4: DCMS to identify and appoint a Senior Responsible Owner to lead on digital continuity**

4.7 The Government Knowledge and Information Management Network (GKIMN) has provided guidance on developing a good KIM structure: *Information Matters: building government's capability in managing knowledge and information*.[4] GKIMN has defined a structure of professional skills to support good KIM in an organisation: *Government KIM Professional Skills Framework*.[5] DCMS should use this guidance to enable its information management practices to support delivery of its overall business objectives.

**Recommendation 5: DCMS should use the GKIMN framework to develop roles and responsibilities for knowledge and information management**

**Recommendation 6: DCMS should give a clear corporate message explaining the role that information plays and the value to the organisation of the information that it creates and shares**

4.8 To ensure that risk is managed and capability is raised within government, individual departments need to establish clear ownership and leadership of knowledge and information management. A department's understanding of the need to provide ownership and leadership in these areas can be assessed from the existence of Knowledge and Information professionals

---

[3] http://www.nationalarchives.gov.uk/information-management/our-services/digital-continuity.htm

[4] http://www.nationalarchives.gov.uk/documents/information-management/information-matters-strategy.pdf

[5] http://www.nationalarchives.gov.uk/information-management/gkim/gkim-professional-skills.htm

with responsibility for the development and implementation of relevant policies, procedures, standards, training and tools. DCMS currently has only one focal KIM role, a head of information management and assurance, which combines KIM and information assurance (IA). This post has been filled on a fixed-term contract. The assessment team was not aware of any plans to recruit a permanent replacement, or identify another suitable equivalent role in the long-term. Combining the responsibilities of IA and KIM is to be commended. However, although a fixed-term contract is sufficient in raising awareness of priority KIM and assurance issues, it leaves DCMS vulnerable in terms of addressing the ongoing risks identified in this report and providing continuity for KIM and assurance long term.

**Recommendation 7: DCMS should review and assess resources to enable coordination of its information assurance, information management and records management activities, including the production of appropriate corporate policies, guidance and action plans**

4.9 Given the potential information risk to the department, DCMS needs to ensure that there is regular reporting of progress to the Board once a structure has been agreed for its information assurance and information management activities. The audit committee do prioritise and report on short term risks, but the focus is not on KIM. An agreed set of appropriate performance measures should be developed to ensure progress on all levels, not just information assurance.[6]

**Recommendation 8: DCMS to develop a set of relevant performance measures to plot improvements in IA and KIM and ensure these are reported regularly to the board**

4.10 DCMS is an amalgam of departments resulting from machinery of government changes. Many of those interviewed saw DCMS as a series of departments that happened to be co-located. This contributed to the development of individual working practices rather than subscribing to

[6] The communication and cultural findings in this report could be linked to the Civil Service Values Poll.

corporate policies and practices. From an IA perspective it is very difficult and costly to either mitigate information risks or to exploit information resources where there are no, or very limited, corporate policies and practices. This was reflected across all levels: there was no common view among interviewees of DCMS' core role and responsibilities. A contributory factor may be that DCMS has approximately 20% annual turnover of staff, with many staff seconded from other departments on short-term or temporary contracts.

**Recommendation 9: DCMS should ensure that they have corporate KIM policies and procedures that support its business objectives, and assign clear responsibilities for delivery**

**Information Assets**

4.11 The assessment team was informed during the onsite visit that DCMS had just finished compiling a revised and more detailed information asset register. DCMS is in the process of confirming information asset owners and roll-out of the appropriate training. The information asset register covers both core DCMS and the Government Olympic Executive (GOE), which provides oversight and assurance of the entire Olympic and Paralympic Programme for the London 2012 Games. GOE is fully supportive of and a key stakeholder in *The Record*, the national collections strategy led by The National Archives and established to ensure that a legacy archive of the preparations for and running of the Games will be available to future researchers and historians.

4.12 The revision of the IAR was carried out by the head of information management and assurance. Some of those interviewed by the assessment team expressed the view that all work to support the information asset register would cease if that position fell vacant. Robust succession planning is necessary to ensure that the work on the information asset register continues to be supported, and that the information asset register continues to be updated and its contents verified.

4.13 Although this work represents a positive start, DCMS must continue to ensure it has a full understanding of the department's information assets, what information it holds, and its potential value to the department.

4.14 Without a full understanding of how the information produced today is critical to the future, the widely held perception that information created has only a short life span as part of a project life cycle will continue to prevail. There needs to be timely consideration of what information should be retained past the end of a project and in what format so that it is accessible and is a full record of the decision-making process.

**Recommendation 10: DCMS should continue to support the work in extending and updating its information asset register**

**Risk management**

4.15 The lack of corporate ownership of knowledge and information management in DCMS means the department has yet to fully identify the risks associated with managing and safeguarding the information it holds and creates.

4.16 Notification of information risks at senior management level is via the audit committee. The Information Services division has a separate risk register, but this only identified IT-related risk and at a rudimentary level. These risks are reported quarterly. However, there was no evidence that information risk was being fully identified and communicated beyond information security. DCMS needs to ensure that all information risks are managed and mitigated appropriately.

4.17 The assessment team have been advised that subsequently work has commenced on identifying and managing information risk. DCMS needs to ensure that ongoing identification, management and mitigation of information risk is continued.

**Recommendation 11: DCMS needs to ensure that there is continuing development and support for the management of information risk in the department**

4.18 DCMS does have a senior information risk owner (SIRO), a role that has had several incumbents. This role needs to be given the authority,

security of tenure and profile within DCMS to effect change. The SIRO needs to be seen as the corporate champion for good information management, and should regularly report to the board on information risk. Guidance on managing information risk for government is detailed in *Managing Information Risk: A Guide for Accounting Officers, Board Members and Senior Information Owners*.[7]

**Recommendation 12: DCMS to raise the profile of the SIRO and reinforce the importance of the role**

4.19 In the wake of the 2009 Data Handling Review, DCMS took the position that there was little that it needed to do to manage its information risks. Many of those interviewed echoed this view, stating that DCMS held very little personal information and was therefore a low-risk department. While senior management have recognised that what personal information is held by the department should fall within its security remit, little overt value has been placed on its corporate business information and other categories of sensitive information.

**Recommendation 13: DCMS should ensure compliance on the handling and storage of business-critical information**

4.20 Although access restrictions can be applied to sensitive information held on LiveLink the assessment team found evidence that in some instances this was not being done. While the need to protect personal information was generally understood, the assessment team was advised, for example, that negotiations on Football Association contracts had not been 'ring-fenced' by the system and had not been recognised as personal or sensitive information and protected accordingly. Staff were either not aware of the potential reputational risk to DCMS of a breach of confidentiality regarding this information or expressed the view that they trusted DCMS colleagues to behave appropriately.

4.21 With an annual staff turnover of approximately 20%, an increased cache of contractors working in high-profile areas such as the Olympics and the risk this carries, plus minimal KIM/IA training for new and existing

[7] http://www.nationalarchives.gov.uk/documents/information-management/information-risk.pdf

staff, this cumulative effect poses a significant information risk.

4.22 DCMS has a duty to properly protect all sensitive information, whether personal or not, and this was not the case. DCMS needs to ensure compliance. All staff should be made aware of their responsibilities with regard to safeguarding sensitive information and the appropriate use of access permissions on LiveLink.

**Recommendation 14: DCMS must investigate the access to personal and sensitive information as a matter of urgency and report to the board on how personal information is protected on LiveLink in line with the Data Handling Review's mandatory minimum measures**

4.23 DCMS cannot manage, exploit or safeguard information holdings that have no structure or appropriate governance. Although implementing this would require effort, once running less ongoing effort would be required, in contrast to the current system where the focus is on fire fighting rather than improvement and progress.

## Records management

> 'I will ensure that our information is appropriately captured, managed, preserved and secure' Jonathon Stephens[8]

5.1 The lack of information management controls in DCMS, with minimal corporate oversight of transfer or appraisal of records, brings the department close to noncompliance with its obligations under the Public Records Act 1958 and the Section 46 Records Management Code of Practice. Adherence to the Public Records Act is mandatory.

5.2 DCMS should make full use of the advice, support and guidance from The National Archives, GKIMN and others to ensure that it achieves compliance and fosters a full understanding of the risks to the department of non-compliance.

### 'What to Keep' synergy

5.3 DCMS has a definition of what is business critical information. However, it has not fully defined the value of the information it creates so it knows from the onset what information it needs to keep. DCMS is in the early stages of checking that this definition is consistently applied. DCMS must consider all of its information holdings to ensure information that has inherent business value, including audit trails of decision-making processes, and information that may be integral to the history of DCMS can be captured and adequately protected. DCMS faces the real risk that key information being created will be lost as it does not understand its value. This creates the real possibility that important information may not be available after the event. Individual business areas have taken local decisions on what should be kept. The department needs to disseminate understanding of the key information for all its service areas and ensure that this is translated into the corporate memory. DCMS must be assured that it has identified its key information assets and that all of these are recorded and assigned an owner.

[8] Permanent Under Secretary Statement of Commitment, 24 February 2010

5.4 Although there were many examples of good local practices, DCMS does not have assurance that local policies and practices are working. DCMS should take steps to address comprehensively what information is business-critical and the value of this information to the department. Until that time there is and will continue to be a substantial risk to the corporate memory of DCMS and a risk that the department will not protect all its business-critical information in an adequate manner.

5.5 DCMS is not currently engaged with The National Archives' What to Keep project. This project helps government departments define what information is business-critical within an organisation and should therefore be retained.

5.6 DCMS, through their DRO, should share good practice internally and identify what information is business critical. The department should also work with the Cabinet Office's Information Assurance and Security (IS&A) team to ensure that the information risks are effectively managed.[9]

**Recommendation 15: DCMS, through their DRO, should work closely with The National Archives' What to Keep project to fully address its business critical information**

**Recommendation 16: DCMS should work closely with IS&A to manage its information risks**

5.7 The Government Olympic Executive (GOE) was a notable exception to the inconsistent understanding within DCMS of information's importance in the running of the business. The GOE has clear business drivers that make it imperative to keep and organise project information. The project status of GOE meant that there were clear timescales and deliverables. However, there was no assurance across DCMS as a whole that staff were clear on what information was business-critical and should be kept, and there was no assessment of the information risks at a corporate level.

[9] Now the Government Security Secretariat

5.8 The Olympics programme has invested in a part-time resource to manage the majority of its records. However, although records are being saved, there is no evidence that there has been either an audit or systematic check to ensure that the full Olympic history is being retained. This is required to ensure that an assessment of the information risks pertaining to the Olympic records is substantiated and documented.

5.9 DCMS needs to ensure that it is satisfied that all relevant project and decision making information will be available once the Olympics has been delivered. Once DCMS has made a corporate decision on what to keep this will go some way to alleviating this issue and provide real benefit to this and other projects.

**Recommendation 17: DCMS should develop a compliance-checking process for GOE in the short term and share this process across the rest of the department**

**LiveLink**

5.10 LiveLink is the primary system for the storage of electronic documents and records for DCMS. LiveLink has been in use since October 2007. It was introduced to business areas with a number of specialist support roles, called information champions, who were seen as the first point of contact for LiveLink queries and creators of new folders.

5.11 A number of those interviewed described difficulties retrieving information. Staff stated that they felt the system was unreliable and not intuitive. Interviewees felt that LiveLink was prone to crashing and that files could be lost from the system. Problems were also perceived with attaching documents from LiveLink, version control and duplication. Some of this was due to staff not having user training or not being aware of some of the functionality of LiveLink. This lack of confidence for whatever reason and the perceived faults of the system has created an environment where many staff circumvent or do not use LiveLink. Staff admitted sending attached documents rather than links and using their desktops, shared drives and personal drives to both draft and store information. The assessment team was advised during interviews that the latter were ‘starting to fill up’. If left unregulated and if the sizes of personal drives are not restricted, there is a risk that business critical information will be

difficult to find. DCMS needs to ensure that there is a clear policy restricting information on personal drives. Staff should be encouraged to delete unnecessary content and move documents to LiveLink.

5.12 While the assessment team found evidence that LiveLink was being underused by some staff, it also found areas that other staff were using it to store too much material. The current version of DCMS' policy on managing electronic information dates from 2004, three years before the introduction of LiveLink. DCMS should ensure that relevant guidance and policies on managing electronic information and the use of LiveLink are reviewed and reissued.

**Recommendation 18: DCMS should review the use of and access to personal drives with a view to supporting effective use of LiveLink**

5.13 There is also concern that unregulated paper copies of documents are being created instead of electronic. This is not sustainable. The greater the options to store information elsewhere, the greater risk that DCMS will not have a definitive version of a document or record which undermines the integrity of the information it holds and does not support informed decision making.

5.14 The assessment team was advised that LiveLink was implemented with limited guidance on naming conventions for new files in the file plan. There is also no limit to the level of hierarchy and only minimum metadata is captured automatically.

5.15 Staff know the information they hold in their area well. However, interviewees advised the assessment team that some searches would recall several thousand results, and finding information outside their work area was identified as a problem by a significant majority. The assessment team is concerned that the minimal metadata requirements captured by LiveLink may not provide sufficient context to assist with more granular advanced searching, although this needs to be analysed. Furthermore, the assessment team is concerned that naming conventions are not uniformly applied at an item level, which may additionally obstruct more useful searching as required by staff interviewed. The assessment team is of the view that the capture of minimum metadata, lack of applied naming

conventions and growing folder structure at business unit level within the file plan may hamper longer-term discovery of information, or understanding if information is required to be transferred across systems, either within DCMS or externally.

**Recommendation 19: DCMS should assess whether current metadata and naming conventions within LiveLink meet long-term requirements for use and discovery and if necessary provide clear guidance on the conventions to be used within it**

5.16 DCMS needs to ensure that there is a continuous programme of training and that a core of 'expert' users of LiveLink is maintained across the department. The expert users must be supported on use of LiveLink and understand data protection principles. These individuals can also provide feedback on LiveLink. This is important to ensure that LiveLink is used effectively and that users' concerns about the system are monitored and responded to. DCMS may wish to refresh the role of the Information Management Champion, to provide the ongoing support that LiveLink requires to support the concept of the 'super user'.

**Recommendation 20: DCMS to identify LiveLink information champion 'super users' and provide appropriate training and support**

5.17 There have been two reviews of the use of LiveLink, the most recent in December 2009, which have highlighted areas where improvement is needed. DCMS should also consider whether LiveLink continues to meet the needs of the department. There does not appear to be a forum to address ongoing issues with LiveLink. There also needs to be consideration of how the information that it already holds would be transferred to a new system, to another department or to The National Archives if the system was no longer to be maintained. This is highly relevant when considering the GOE records. Establishing a LiveLink forum would act as a conduit for such discussions.

**Recommendation 21: DCMS should create a physical or 'virtual' LiveLink forum to improve communication and address common information management issues within the system**

**File plan**

5.18 The file structure used by DCMS is not meeting the needs of the business. The strategic top file levels were defined originally by an external consultant, but the lower file levels have been left for business units to create as required; this has lead to haphazard, unplanned file creation with no overall plan. Good practice recommends a maximum of five levels. Beyond this there is a risk that information will be lost or become orphaned. Staff retain their own memory maps of where they have saved and where to relocate their documents. The assessment team have been advised that DCMS is in the process of reviewing the current file structure to address this.

**Recommendation 22: DCMS should conduct a wider user review to assess user concerns, prioritise these concerns to address what changes to LiveLink can be implemented as appropriate**

5.19 LiveLink needs to be understood as both an information management and records management tool. The head of information management and assurance is well placed to have responsibility in ensuring that the information management capabilities of the system meet business requirements. This will require a close working relationship with IT to enable potential information management issues to be clearly identified and managed with the required technical support and input.

**Departmental records officer (DRO)**

5.20 The GOE has a part-time DRO. DCMS has always had a DRO role defined, but it has at various times been vacant. The most recent DRO has been in post since November 2009. The gaps in assigning this role meant that there was no identifiable strategic policy lead on records management to ensure standards were met, training given, policies and guidance were in place, regularly reviewed and monitored for compliance. The requirement for a DRO follows recommendations made in the Grigg Committee report in 1954. Following this, HM Treasury wrote to each department stating that each department is required to nominate a DRO; this is still the case today.

5.21 A DRO is essential in spreading and instilling good practice within records and information management across DCMS and provides a level of continuity and cohesion for the department on what good information and records management is. Unless sufficient weight and resources are given to this core oversight role, DCMS will continue to fail to meets its obligations in this regard under the Public Records Act and HM Treasury instructions. Failure to keep the relevant information also poses the possibility of DCMS' loss of reputation and potentially risk external intervention by other bodies.

**Recommendation 23: DCMS should assess ongoing resourcing and responsibilities of a DRO to give assurance that the department is fulfilling its KIM obligations**

5.22 There were examples of individuals attempting to share understanding of good information and record management practice, such as transferring information from shared drives into LiveLink, and then restricting access to the previous shared drive. This was at a local level. The current contracted records centre manager has been proactive in raising individual team awareness of retention and disposal of paper files. This action needs to be extended across DCMS.

**Good practice**

5.23 DCMS is not maximising the use of the information that it has. There is no system in place to ensure that best practice relating to all aspects of records and information management is shared. There was good practice in several teams, for example the legal team, web team and GOE, who had a combination of 'Useful Information Areas' and 'Know How' for key documents contained within their team's file structure.

5.24 The legal team was an exemplar in information management. The team's ability to organise and locate information was widely recognised in so far as those other business units frequently approached them for documents that they could not locate in their own file structures. This was evidenced by several interviewees who stated they would speak to the legal team if they were unable to find information that they needed. The team have already offered to share their expertise in information management practice across DCMS. As this system works it may be

possible to translate it to other areas of DCMS.

**Recommendation 24: DCMS should look at and learn lessons from areas where KIM expertise was been successfully implemented and use that expertise to build similar capability in other business units**

### Records centre

5.25 The records centre database holds information on all the paper files and their contents that have been sent for external storage. This database is an effective system for tracking and retrieving the exact file when required, removing the need to retrieve several files at once and minimising the cost of retrieval to DCMS. However, although the database is present on the departmental IAR and a link to it can be found on the records centre intranet pages, interviewees were not generally found to know of its existence. The database may not be utilised to its full potential as a corporate resource.

5.26 The records centre database is held on an Oracle-based system. There does not appear to be a specific plan in place to retain or transfer the information held on it should the database no longer need to be maintained.

**Recommendation 25: DCMS to consider ongoing access to the records centre database as part of long-term information management strategy**

### File review

5.27 DCMS has a contract with Ecovert for the provision of services internally to review files ready for transfer to The National Archives. Currently, there are two people covering this function for DCMS. This role is critical in ensuring that the appropriate records are selected for DCMS' legacy and in ensuring that DCMS meets its obligations over the forthcoming transition period after the reduction from thirty to twenty years. Although Ecovert are contracted to provide skilled staff to do the reviews, there is a risk that DCMS itself has not invested in ensuring that it has the skills internally to either support or carry out this function in the event that there is gap in Ecovert's service provision.

**Recommendation 26: DCMS to assess and mitigate the risks needed to identify staff with the skills and knowledge to conduct file review**

**Recommendation 27: DCMS should, for consistency in records appraisal, ensure that it has experienced staff knowledgeable in its business managing the review process**

5.28 At the time of assessment, the management of the storage, retrieval and review contract was not the responsibility of the DRO or head of KIM, but was a function covered by the DCMS property team. The head of information management and assurance, acting as DRO, now has an oversight role of this contract. Despite having performance indicators in place there has not been any compliance checking.

**Recommendation 28: DCMS to implement a programme of compliance checking to ensure that the contractor service provided is the level required**

**Recommendation 29: DCMS to ensure there is a continuity plan in place for the management of the store and the review of paper files should contractual arrangements change**

5.29 DCMS has a contract with Iron Mountain that covers off-site storage of registered paper files. The assessment team note that there has been recent progress in reducing paper files in storage which has delivered cost savings to DCMS.

**Retention**

5.30 A blanket retention review has been created for all files in LiveLink. Once created, top-level folders are flagged for further review. No such review was attached to the lower level sub-folders. There is the potential to create a problem for DCMS if several thousand records in LiveLink are flagged for review at the same time. The assessment team was advised that this has the potential to crash the DCMS system.

5.31 Without an understanding of when documents should be reviewed,

retained or destroyed, this decision is not based on what information is critical to DCMS. DCMS is at risk of breaching the Data Protection Act and Freedom of Information legislation by retaining information for longer than it should. The assessment team found evidence that paper records were also retained longer than required. Without clear guidance on retention and disposal of documents, DCMS is exposing itself at all levels to external scrutiny.

5.32 DCMS needs to ensure that retention schedules are set for each individual business area and that there is a corporate oversight role to give assurance that these schedules are universal. If DCMS does not create retention schedules for the areas that do not posses them, the ever increasing volume of documents in LiveLink will become unsustainable. This will make retrieval of information time consuming and cause DCMS to be at risk of DPA and FOI disclosure issues.

**Recommendation 30: DCMS to develop an appropriate retention policy applicable to all business areas and encompassing all document record formats**

**Recommendation 31: Compliance checks to be scheduled to assess the coverage and effectiveness of the resulting retention schedules**

**Transfer**

5.33 DCMS selects documents for transfer to The National Archives by mirroring the Grigg system for the first and second review. This system, without the necessary retention schedules, is too rigid and not effective for the needs of DCMS. Staff can schedule files for destruction at an earlier or later point if they feel it appropriate but DCMS cannot have full assurance over this process. DCMS needs to develop its own appraisal system, and ensure that this is communicated across DCMS, along with associated training. This will enable confidence by internal businesses that the relevant records are disposed of and records sent to The National Archives are the appropriate ones.

**Recommendation 32: Working with The National Archives, DCMS should develop an appraisal system for paper and electronic records, and a programme of training to support implementation**

**Digital continuity**

5.34 DCMS needs to take active steps to ensure the continuity of its digital information. Digital information, irrespective of its format, poses unique problems for organisations, which need information to be both reliable and available. Loss of digital continuity for departments such as DCMS is a key information risk. DCMS has been subject to several machinery of government changes which may impact on its ability to use information over time. The risks to maintaining the completeness, availability and usability of that information increase over time.

5.35 In common with many other government organisations, there is already evidence to suggest a loss of digital continuity within the organisation, and there are potential continuing risks to the information it holds. For example, the web content management system was transferred between Microsoft (FrontPage) and Red Dot in 2009. When doing so, much of the original file structure was not maintained during the transfer. Both management systems now have to be maintained at additional cost to DCMS as the Microsoft system needs to be referred to when files cannot be found within Red Dot. If there had been timely consideration of migration plans that covered the usability required from the system this could have been avoided. Potential savings in time and resources could have been made with the Web team not having to continually refer across two systems. A further example can be found in the photographic files from the Millennium Dome which were transferred from the New Millenium Experience Company, a non-departmental public body of DCMS, to The National Archives. These were found to be disorganised and without description of content and some were unreadable. Contextual metadata needs to be re-keyed and the availability and usability of some files has been lost. This should have been mitigated against if the information had been well characterised and requirements understood.

5.36 Understanding of digital continuity as an information risk appears to be at a personal, rather than at a corporate or strategic level within DCMS. The root cause is again the absence of a coherent corporate

understanding of information, its risks and its management. Although DCMS was one of the original funding departments for the National Archives' Digital Continuity project, the department is not currently engaging with the project. DCMS does not have a senior responsible owner (SRO) for digital continuity, nor any strategy or action plan to manage continuity. Within DCMS the responsibility could be within the role and responsibilities of head of KIM or equivalent senior level post, with the support of both the SIRO and chief information officer (CIO) at board level. Both the SIRO and CIO need to ensure they are aware of digital continuity risks and issues within DCMS, and that they have read the appropriate guidance from The National Archives and are committed to managing issues within DCMS.

5.37 To effectively manage the digital continuity process, the SRO should form a cross-team working group, initially comprised of members with the authority and responsibility to develop a digital continuity strategy and align it within a wider information management strategy for DCMS. It is advisable that this group should cover responsibilities within the information technology, information assurance, business change and information management functions. DCMS should also involve their IT suppliers.

5.38 DCMS needs to start building a digital continuity action plan following the guidance laid out in Managing Digital Continuity, with the assistance of The National Archives.[10]

**Recommendation 33: DCMS to form a cross-working project team to define digital continuity for the department and develop a digital continuity strategy and subsequent action plan**

**Recommendation 34: DCMS should detail its digital continuity risks in its information assurance risk register**

[10] http://www.nationalarchives.gov.uk/documents/information-management/managing-digital-continuity.pdf

### Email

5.39 The current DCMS email policy is listed in the department's 2004 policy on managing electronic information. Limits on inbox size are in place but staff decide what information to keep and delete. DCMS needs to ensure that emails that are critical to the business are kept and are accessible. DCMS is again vulnerable to DPA and FOI as a result of not defining expectations and responsibilities. The policy must state how this is communicated. DCMS needs to ensure that there is compliance to this policy once implemented. In order to be properly enforced this policy should be signed off at board level to give it due weight.

**Recommendation 35: DCMS should develop and implement an appropriate email policy that is coherent with other KIM requirements**

### Library services

5.40 Book loans are available to staff on request via the DCMS library. This can no longer be easily browsed by staff. Journals are made available to staff via the 'Info Point'. A number of the paper library resources have been reduced and electronic subscriptions increased. The progress made towards rationalising library resources should be commended. However, the library and its resources do not appear to be included in the information management resources for DCMS. A library is a core element of a holistic information management approach within a department. DCMS needs to ensure that this area of responsibility is allocated within the remit and functions of the head of KIM or similar equivalent role. Combining responsibility for information resources helps provide a wider focus for reuse of that information. Without this line of responsibility, changes to the library and access to information may also be disjointed and uncoordinated.

5.41 There may be value in DCMS attending meetings with other heads of KIM in government to assess where large savings can be made in purchasing electronic subscriptions in the longer term.

**Recommendation 36: DCMS to ensure that responsibility for the library resources are allocated within the remit/functions of knowledge and information management**

## Access to information

6.1 The absence of a comprehensive corporate compliance-checking regime in DCMS has made it vulnerable on many fronts. The current internal audit programme does not assess how various processes across DCMS work. Where policies, guidance and even contracts relating to records and information management are in place, there has been little or no checking of implementation, adherence to guidance or standards. The assessment has evidenced that DCMS has a number of potentially serious gaps that once added together provide evidence that it is at risk of reputational and possible legal challenge as it cannot demonstrate a full programme of legislative compliance across the department. This is pertinent for DCMS where these do not fall readily within the annual audit schedule for example where they do not meet obligations under the Public Records Act, Data Handling Review or meet accepted best practice standards or codes of practice such as the Lord Chancellor's Code of Practice on the Management of Records.

6.2 DCMS has to ensure that where there is an obligation to meet statutory and other guidance it does so, throughout the department. Without a robust compliance mechanism that both supports and feeds into audit activities DCMS will continue to risk its reputation and undermine its performance. Compliance checks also enable the department to assess the parts of the business that are doing well, where systems are failing or where guidance provided is unclear. DCMS should try to preserve resources, it may be beneficial if some of the compliance checking activities is integrated or run in tandem within the annual programme of internal audit activity. The head of information management and assurance would oversee the KIM activities that feed into the compliance checking.

**Recommendation 37: DCMS should coordinate compliance-checking activities so that these support and feed into internal audit**

**Recommendation 38: The resulting integrated compliance-checking audit programme is reported to the board at regular intervals**

6.3 There is a real and continuing risk that information that needs to be safeguarded is not. Of those interviewed, there was no clear understanding of the Government Protective Marking Scheme. For instance, one team stated that staff were 'trusted' to safeguard the information, rather than having explicit knowledge and guidance on what information needs to be safeguarded and the appropriate access restrictions. DCMS must ensure that all staff whether contract or permanent are aware of and correctly apply protective markings, and that there are processes in place to check compliance.

6.4 Data Protection Act/Freedom of Information and protective marking training is a statutory obligation and therefore has to be a corporate responsibility. DCMS needs to ensure that training/information sessions are attended by all. In a department where many staff are on contracts or are temporary workers this is particularly critical.

**Recommendation 39: DCMS should institute a rolling programme of refresher training on protective marking, which should also extend to staff on secondments and contractors**

**Recommendation 40: Induction training should include protective marking training for new starters**

6.5 The assessment team have subsequently been advised that since April 2010, protective marking training is now included in the e-learning induction package.

**Data Protection Act 1998**

6.6 There was some understanding of what constituted personal information, demonstrated by limited staff awareness of the Data Protection Act (DPA), but this was not universal. The assessment team noted a lack of understanding of how DPA affected potentially sensitive information beyond names and addresses, for instance sensitive information relating to arrangements for the visits of senior politicians and heads of state were not fully protected from accidental disclosure to third parties. This is a potentially serious risk for DCMS to its national and international reputation and credibility.

**Recommendation 41: DCMS to ensure that there is an ongoing training programme for DPA for all staff within specialist and non-specialist business areas**

### Freedom of Information

6.7 DCMS answers all Freedom of Information (FOI) requests through the Public Response and Engagement Unit (PERU). This unit coordinates and fields departmental responses to FOI requests. The staff in PERU do not appear to have an oversight function for the quality of the information that is sent back from subject business areas. There have been questions raised regarding the integrity and quality of information released under FOI requests. The assessment team was unable to ascertain the level of training that local staff had to ensure the accuracy and completeness of replies, or that relevant exemptions are applied.

6.8 DCMS needs to satisfy itself that it has provided clear guidance and that the importance of FOI is understood at all levels. DCMS must ensure that any corporate guidance is produced and made mandatory for all. In areas such as human resources, DCMS must engender confidence that its staff have the knowledge and the tools to comply with DPA and FOI and also have a definitive point of contact to raise any issues or concerns.

**Recommendation 42: DCMS to ensure that there is a comprehensive training programme for FOI for all relevant staff within specialist and non-specialist business areas**

### Reuse

6.9 There are areas in DCMS where the reuse of information is well established. DCMS has a positive relationship with certain external partners on how it should and could reuse some of the myriad cultural data that it holds and generates. The assessment team was made aware that DCMS organised a Rewired Culture event that took place on 27 March 2010.[11] This event brings together users and data owners to explore what can be done with the information and discuss challenges.

[11] http://rewiredstate.org

6.10 DCMS does not just create information internally. For example, some teams commission external surveys such as survey data commissioned by analysts. There is no policy on who should own or be able to exploit the information. DCMS should centrally record its survey data and share it where possible. This will avoid duplication of effort in sourcing information and wasting resources by commissioning the same or similar surveys.

6.11 DCMS should assess what information it holds and can make more widely available for re-use. It should work with The National Archives to ensure that data is made available online at data.gov.uk.

**Recommendation 43: DCMS to continue working with The National Archives to identify what information could be made available on data.gov.uk**

## Compliance

### Change management: One DCMS

7.1 DCMS is working to build a sense of one department working towards a common purpose. It has four strategic business objectives published on its website which clearly set out the department's aims, but only one member of staff interviewed could give DCMS' strategic business objectives, others listed the objectives of their own business unit.

7.2 Many sub-environments exist within DCMS which reflect the values of individual business unit leaders and do not support consistency of practice or corporacy of working practices. Information and information management are key to achieving change, contributing to and supporting the business objectives.

### Hot-desking

7.3 DCMS will shortly be giving up floor space in its building and moving to 'hot-desking' with specific areas assigned to this. This will result in a reduction of space to store physical information. There are general 'house rules' to ensure, for example, that staff do not leave restricted information unlocked, and most staff have access to the information they need electronically. DCMS needs to ensure that the contents of files sent to offsite storage, for example, Iron Mountain, is referenced appropriately, to ensure that files are properly recorded to aid future retrieval. To ensure business critical information is not lost, DCMS must also ensure oversight of any disposal of paper records that occurs as a result of the move to hot-desking.

### Staff responsibilities: information champions

7.4 With the Introduction of LiveLink, DCMS created a number of Information Management Champions. This role was initially identified as pivotal in providing support to teams in managing and coordinating the file structure for LiveLink. Information Management Champions were also intended to provide support for minor technical issues with the system.

7.5 The Information Management Champion role is not assigned to a particular grade. The assessment team was advised that this could create difficulties if the behaviours of more senior staff in relation to information management had to be challenged. DCMS needs to ensure that all managers are aware of their responsibilities in both managing the Information Management Champions and leading by example by following DCMS policy and guidance.

**Recommendation 44: DCMS needs to ensure that all managers are aware of their responsibilities in both managing the Information Management Champions and following records and information management guidance**

7.6 Over time, the Information Management Champion role has largely been reduced to setting up folders on LiveLink. A minority of Information Management Champion provide record management and information management duties for their teams. The low-level of information management and record management compliance in DCMS needs to be addressed. The reinvigorated Information Management Champion role could be used to support DCMS achieving KIM compliance in the department.

7.7 The Information Management Champion role needs to have its responsibilities clearly defined and given the support necessary to carry out the job.

**Recommendation 45: DCMS should set out the responsibilities of the Information Management Champions to ensure that their role and the governance structure is endorsed by the DCMS board**

7.8 There has been an absence of coordination, direction and training for the Information Management Champions. The role is a potential resource to the department that is currently being underutilised. A network for the Information Management Champions was instigated in December 2009. The importance of this was underlined by one interviewee who had attended the initial meeting and expressed surprise at discovering that other Information Management Champions shared similar problems.

Reinforcing the role and establishing a regular forum will best practice and knowledge to be shared, aiding the establishment of a DCMS-wide KIM discipline.

7.9 The Information Management Champions should form part of the department's KIM governance structure and be given a lead role in ensuring that the business units they are responsible for are compliant. The Information Management Champions should be able to report back on KIM centrally to the Head of KIM function. This refocusing of roles and responsibilities will aid DCMS to manage its limited KIM resources.

**Recommendation 46: Each Information Management Champion should have a clear role description and adequate time and opportunity to fulfil the role**

**Recommendation 47: The Information Management Champion network should be linked to the head of KIM/DRO. The responsibilities of the role should be communicated throughout DCMS**

**Training**

7.10 There have been a number of changes to senior management within HR, which has impacted on the strategic focus of training delivery. If staff are not given clear direction and training, they will develop their own practices to enable them to carry out their tasks, with the resultant lack of consistency and poor practices.

7.11 With the exception of information assurance training which is now mandatory, training in DCMS appears reactive. The assessment team was not aware of any formal, organised and regular information management training as part of an induction programme for new entrants to the department. In a department where many staff are contracted, DCMS must ensure that there is a quick way to ensure that staff fully understand their responsibilities in safeguarding and managing information correctly. Induction training that incorporates information at an early stage would counter the development of poor practices which cannot easily be reversed.

**Recommendation 48: DCMS to ensure that the induction process for new staff includes KIM and IA training and identifies corporate and local information risks**

**Recommendation 49: DCMS to establish a mandatory programme of targeted briefings/training sessions on KIM and IA for contractors**

7.12 DCMS is currently addressing the ongoing resource and departmental challenges for HR. Once HR has a vision and focus it can provide the priority training and development that DCMS require.

**Polices and guidance**

7.13 DCMS has produced guidance on records management entitled *A Guide to Records Management in DCMS*. This was last updated in 2008. The guidance outlines roles and responsibilities for staff in DCMS and makes reference to the roles and responsibilities of the contractor regarding paper records. The guidance also outlines specific responsibilities for the DRO role, which was not assigned at the time of the assessment. There was no evidence that DCMS carries out internal compliance checks on adherence to the policy. In addition, while the guidance is comprehensive, it is not considered to be user-friendly, so staff either ask a colleague or develop their own local solutions. DCMS needs to produce guidance that is up to date, addresses the section 46 Records Management Code of Practice, is user-friendly and is easily accessible to all.

**Recommendation 50: DCMS should assign ongoing responsibility for ensuring that KIM guidance is reviewed and updated periodically**

## Culture

### Management

8.1 Senior management are key to engendering good information management practice. An informed supported management tier would be able to drive the necessary changes through their own staff and, ultimately, the department as a whole. Without the support and understanding of managers, the changes needed throughout DCMS to raise standards and awareness of good KIM practices will be at best limited and at worst ineffective.

**Recommendation 51: DCMS to develop a programme of targeted KIM awareness sessions for managers**

### Information sharing

8.2 There is limited sharing of information, resources and knowledge across DCMS. This makes duplication of information and effort highly likely. The assessment team was advised that compilation of the revised IAR had enabled the discovery of a number of mailing lists, contacts, networks, non-personal research and surveys that potentially could be shared more widely and bring benefit across DCMS. Knowledge sharing can help avoid wastage through duplication. Where duplication occurs there is the real possibility that resources are not being used in the most efficient and effective way and information that should be is not being adequately protected.

### Staff awareness

8.3 DCMS has a wealth of truly committed and enthusiastic staff dedicated to their own business objectives. In general, staff were found to value the information they created and held locally. However, this value usually did not extend to ensuring that it was saved for the corporate memory, adequately protected and exploited, as demonstrated by the widespread storage outside LiveLink.

8.4 The assessment team identified a number of staff who had been in a particular role for a significant number of years and with knowledge and

expertise unique both to them and their role. Although some of their accumulated ‘know-how’ was captured in LiveLink much of it was not. The danger exists that when they leave the department there will be a serious knowledge gap that cannot be easily filled, which will significantly impact on the department’s ability to conduct some of its core functions.

**Recommendation 52: DCMS should identify staff whose knowledge and expertise are of significance to meeting the department’s business objectives and consider how it can best use this expertise**

### Knowledge transfer

8.5 No active knowledge transfer was found for staff leaving DCMS, or moving on loan or secondment. Exit interviews were found to be available on request only. This is a significant risk, as staff can move or leave suddenly without the opportunity to pass on their knowledge unless a formal system for its transfer is in place.

8.6 Key decisions and work practices need to be saved and auditable. Whilst some of this information may be saved locally, there should be a considered corporate approach to ensuring that as staff leave, there are mandated mechanisms in place to enable a handover of their knowledge and information. Without this, DCMS is at risk that key information, such as that stored on personal drives and email, will be lost once the postholder has left.

**Recommendation 53: DCMS should develop and implement a formal policy to capture knowledge within a structured handover process for leavers and movers**

**Recommendation 54: DCMS should plan to undertake a knowledge-harvesting exercise to ensure that when key staff with specialist skills or knowledge leave the department, essential information relating to their roles is stored**

### Knowledge management

8.7 Knowledge and information management in DCMS is at an immature

stage. The lack of strategic direction and ownership of KIM has led to a department that is functioning on a general day-to-day basis, with staff being trusted to manage and do the right thing. If this trust is broken, the risk for DCMS is that there is no structure to ensure business continues and this could lead to dysfunction.

8.8 Knowledge and information is not shared and there is no sense of purpose ‘as one’. Staff need to be and feel engaged with DCMS. There is a wealth of professional commitment and knowledge that is not being utilised. Taking a structured, strategic approach to knowledge and information management will enable DCMS to begin to plan to address the issues raised in this report. With that will be the assurance that they are keeping the correct information, setting the standards by which this will be achieved and are meeting their statutory obligations.

# 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 agreed, will form an action plan that will be monitored.

| Business area | Ref | Recommendation |
|---|---|---|
| Governance | 1 | DCMS should identify how to position information management strategically in DCMS and provide the appropriate support, resources and guidance at board level to achieve this |
| | 2 | The board should designate a senior champion to have corporate responsibility for KIM |
| | 3 | The role with overall responsibility for KIM should lead on developing the long-term vision and plan for KIM for DCMS |
| | 4 | DCMS to identify and appoint a Senior Responsible Owner to lead on digital continuity |
| | 5 | DCMS should use the GKIMN framework to develop roles and responsibilities for knowledge and information management |
| | 6 | DCMS should give a clear corporate message explaining the role that information plays and the value to the organisation of the information that it creates and shares |
| | 7 | DCMS should review and assess resources to enable coordination of its information assurance, information management and records management activities, including the production of appropriate corporate policies, guidance and action plans |
| | 8 | DCMS to develop a set of relevant performance measures to plot improvements in IA and KIM and ensure these are reported regularly to the board |
| | 9 | DCMS should ensure that they have corporate KIM policies and procedures that support its business objectives, and assign clear responsibilities for delivery |
| | 10 | DCMS should continue to support the work in extending and updating its information asset register |

| | | |
|---|---|---|
| | 11 | DCMS needs to ensure that there is continuing development and support for the management of information risk in the department |
| | 12 | DCMS to raise the profile of the SIRO and reinforce the importance of the role |
| | 13 | DCMS should ensure compliance on the handling and storage of business-critical information |
| | 14 | DCMS must investigate the access to personal and sensitive information as a matter of urgency and report to the board on how personal information is protected on LiveLink in line with the Data Handling Review's mandatory minimum measures |
| Records Management | 15 | DCMS, through their DRO, should work closely with The National Archives' What to Keep project to fully address its business critical information |
| | 16 | DCMS should work closely with IS&A to manage its information risks |
| | 17 | DCMS should develop a compliance-checking process for GOE in the short term and share this process across the rest of the department |
| | 18 | DCMS should review the use of and access to personal drives with a view to supporting effective use of LiveLink |
| | 19 | DCMS should assess whether current metadata and naming conventions within LiveLink meet long-term requirements for use and discovery and if necessary provide clear guidance on the conventions to be used within it |
| | 20 | DCMS to identify LiveLink information champion 'super users' and provide appropriate training and support |
| | 21 | DCMS should create a physical or 'virtual' LiveLink forum to improve communication and address common information management issues within the system |
| | 22 | DCMS should conduct a wider user review to assess user concerns, prioritise these concerns to address what changes to LiveLink can be implemented as appropriate |
| | 23 | DCMS should assess ongoing resourcing and responsibilities of a DRO to give assurance that the department is fulfilling its KIM obligations |
| | 24 | DCMS should look at and learn lessons from areas where KIM expertise was been successfully implemented and use that expertise to build similar capability in other business units |
| | 25 | DCMS to consider ongoing access to the records centre database as part of long-term information management strategy |
| | 26 | DCMS to assess and mitigate the risks needed to identify staff with the skills and knowledge to conduct file review |

| | | |
|---|---|---|
| | 27 | DCMS should, for consistency in records appraisal, ensure that it has experienced staff knowledgeable in its business managing the review process |
| | 28 | DCMS to implement a programme of compliance checking to ensure that the contractor service provided is the level required |
| | 29 | DCMS to ensure there is a continuity plan in place for the management of the store and the review of paper files should contractual arrangements change |
| | 30 | DCMS to develop an appropriate retention policy applicable to all business areas and encompassing all document record formats |
| | 31 | Compliance checks to be scheduled to assess the coverage and effectiveness of the resulting retention schedules |
| | 32 | Working with The National Archives, DCMS should develop an appraisal system for paper and electronic records, and a programme of training to support implementation |
| | 33 | DCMS to form a cross-working project team to define digital continuity for the department and develop a digital continuity strategy and subsequent action plan |
| | 34 | DCMS should detail its digital continuity risks in its information assurance risk register |
| | 35 | DCMS should develop and implement an appropriate email policy that is coherent with other KIM requirements |
| | 36 | DCMS to ensure that responsibility for the library resources are allocated within the remit/functions of knowledge and information management |
| Access to Information | 37 | DCMS should coordinate compliance-checking activities so that these support and feed into internal audit |
| | 38 | The resulting integrated compliance-checking audit programme is reported to the board at regular intervals |
| | 39 | DCMS should institute a rolling programme of refresher training on protective marking, which should also extend to staff on secondments and contractors |
| | 40 | Induction training should include protective marking training for new starters |
| | 41 | DCMS to ensure that there is an ongoing training programme for DPA for all staff within specialist and non-specialist business areas |
| | 42 | DCMS to ensure that there is a comprehensive training programme for FOI for all relevant staff within specialist and non-specialist business areas |
| | 43 | DCMS to continue working with The National Archives to identify what information could be made available on data.gov.uk |

| | | |
|---|---|---|
| Compliance | 44 | DCMS needs to ensure that all managers are aware of their responsibilities in both managing the Information Management Champions and following records and information management guidance |
| | 45 | DCMS should set out the responsibilities of the Information Management Champions to ensure that their role and the governance structure is endorsed by the DCMS board |
| | 46 | Each Information Management Champion should have a clear role description and adequate time and opportunity to fulfil the role |
| | 47 | The Information Management Champion network should be linked to the head of KIM/DRO. The responsibilities of the role should be communicated throughout DCMS |
| | 48 | DCMS to ensure that the induction process for new staff includes KIM and IA training and identifies corporate and local information risks |
| | 49 | DCMS to establish a mandatory programme of targeted briefings/training sessions on KIM and IA for contractors |
| | 50 | DCMS should assign ongoing responsibility for ensuring that KIM guidance is reviewed and updated periodically |
| Culture | 51 | DCMS to develop a programme of targeted KIM awareness sessions for managers |
| | 52 | DCMS should identify staff whose knowledge and expertise are of significance to meeting the department's business objectives and consider how it can best use this expertise |
| | 53 | DCMS should develop and implement a formal policy to capture knowledge within a structured handover process for leavers and movers |
| | 54 | DCMS should plan to undertake a knowledge-harvesting exercise to ensure that when key staff with specialist skills or knowledge leave the department, essential information relating to their roles is stored |

# APPENDIX TWO: IMA COMMITMENT

I am personally committed to ensuring that we create and manage the information we need to fulfill our corporate obligations. To show the strength of my commitment, I have asked The National Archives to assist us in conducting a review into our information management processes.

Information is recognised as a key asset for running our business effectively and I will ensure that our information is appropriately captured, managed, preserved and secure.

The Department for Culture, Media and Sport supports this commitment in practice and I look forward to receiving their report and working with The National Archives to further develop our information management capability.

Jonathan Stephens

Permanent Secretary

## APPENDIX THREE: GLOSSARY

| | |
|---|---|
| IA | Information Assurance |
| IAR | Information Asset Register |
| BIS | Department for Business, Innovation and Skills |
| CIO | Chief Information Officer |
| DCMS | Department for Culture, Media and Sport |
| DPA | Data Protection Act |
| DRO | Departmental Records Officer |
| FOI | Freedom of Information |
| GKIMN | Government Knowledge and Information Management Network |
| GOE | Government Olympic Executive |
| IM | Information Management |
| IMA | Information Management Assessment |
| IRR | Information Risk Return |
| IT | Information Technology |
| KIM | Knowledge and Information Management |
| NDPB | Non Departmental Public Body |
| PERU | Public Engagement Responsibility Unit |
| PQs | Parliamentary Questions |
| SIRO | Senior Information Risk Owner |
| SRO | Senior Responsible Officer |