CIVILSERVICE

Information Management Assessment

Department for Transport
June 2009

The National Archives

PART ONE: EXECUTIVE SUMMARY

1. The Department for Transport's policies and practices in terms of Information Assurance are very strong. It should be noted that DfT has led firmly from the front on the implementation of the Data Handling Review over the past year. The Permanent Secretary has been instrumental in communicating a strong message throughout the organisation, reinforcing and informing the need for effective data handling and data security procedures. The culture has been transformed and good data handling has become the norm, not the exception.

2. DfT is building on this progress to push forward the programme to embed sound information management policies and procedures across the organisation. Firm commitment from the lead Director General and senior management is central to this drive and vital in reinforcing the practices DfT is implementing. Changing the culture of the organisation is not going to happen instantly, but it can be achieved effectively if staff feel engaged and involved in the process. DfT recognises this.

3. Following on from its successful work on information assurance, the Department is in the process of developing a knowledge and information management strategy that will change the way DfT works considerably. DfT has recognised the need to move forward, challenge the current culture and embed good information management practices across the organisation to achieve well informed policy creation and development.

4. An important theme of the knowledge and information strategy is to improve the Department's processes for record management. The priority here should be to determine what corporate information DfT should be keeping. DfT recognises that it needs to make more progress in this area. The risk of not capturing key critical business information in any organisation has significant legal, financial and reputational consequences.

5. The knowledge and information management strategy should inform

and determine exactly how DfT will manage its information and knowledge assets. Once DfT is certain about what it should keep, it should then consider how it should be kept.

6. The central department's records management function is provided under a service level agreement with the Department for Communities and Local Government. This contract is well maintained and monitored and provides a good quality of service to DfT. However, DfT now needs to take ownership of its information and records management strategy so the organisation can develop and champion its own policies. The need for a strategic lead on this is clear. The appointment of a Deputy Director within the Information Management Directorate to develop a strategy is a commendable first step.

7. DfT is in the process of instigating a culture change around information management. This report and its recommendations address a number of areas on which DfT should focus to assist with the change process. The National Archives would encourage DfT to implement these recommendations, with the support of The National Archives, in order to become an effective knowledge sharing and information exploiting organisation.

8. Since the on-site assessment in June 2009, The National Archives are pleased to note that the central Department for Transport have implemented a number of solutions to address some of the findings of the report, and that the strategies highlighted above include measures to address a number of findings of this report.

Risk Matrix

Governance

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

Records Management

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

Access

FOI/Data Protection		Best Practice
Re-Use		Good
Security		Best Practice

Compliance

Staff responsibilities and delegations		Good

Policies and guidance		Satisfactory
Training		Development needed
Change management		Good

Culture

Commitment		Good
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

9. 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.

10. 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.

11. 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.

12. 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.

13. This report sets out the findings, conclusions and recommendations of The National Archives' IMA Assessment of the central Department for Transport (DfT(C)).

The Business of the Department for Transport (DfT)

14. The Department for Transport is a department of state providing leadership across the transport sector to achieve its objectives, working with regional, local and private sector partners to deliver its services.

15. The central department employs around 2,000 staff. Over 350 work in front-line units, including transport security and the marine, air and rail accident investigation branches. Most staff are based in London, with others in Hastings, Farnborough, Southampton and Derby. The Department's total administration cost is budgeted at £275m for 2009–10.

16. The current Department is the product of a series of mergers and demergers over the last twelve years. The transport function in this time has moved between the Department of Transport, the Department for the Environment, Transport and the Regions (DETR), the Department for Transport, Local Government and the Regions (DTLR) and finally in 2002, the new Department for Transport (DfT).

17. The Department for Transport's aim is transport that works for everyone. This means a transport system that balances the needs of the economy, the environment and society. In support of this aim the Department has five strategic objectives which focus on the core area of its business:

One: To support national economic competitiveness and growth, by delivering reliable and efficient transport networks.

Two: To reduce transport's emissions of carbon dioxide and other greenhouse gases, with the desired outcome of avoiding dangerous climate change.

Three: To contribute to better safety and security, health and longer life-expectancy through reducing the risk of death, injury or illness arising from transport, and promoting travel modes that are beneficial to health.

Four: To promote greater equality of opportunity for all citizens, with the desired outcome of achieving a fairer society.

Five: To improve quality of life for transport users and non-transport users, and to promote a healthy natural environment.

18. The Department has seven executive agencies (employing a further 16,500 staff) to deliver the Government's transport priorities and services. These are the Driving Standards Agency (DSA), Driver and Vehicle Licensing Agency (DVLA), Vehicle Certification Agency (VCA), Vehicle and Operator Services Agency (VOSA), Highways Agency (HA), Maritime and Coastguard Agency (MCA) and Government Car and Despatch Agency (GCDA).

19. A further body, Network Rail, is key to DfT's operations. This company, limited by guarantee, owns and operates Britain's rail infrastructure.

20. The Civil Aviation Authority (CAA), an independent specialist aviation regulator, also works closely with DfT and advises on UK aviation issues.

21. The Department works with the European Commission, the International Civil Aviation Organisation and the International Maritime Organisation which are responsible for an increasing proportion of international transport legislation. The Department also has bilateral relations with numerous other countries.

Information Management at the Department for Transport

22. The records management service at the DfT(C) is provided under a shared service SLA agreement with the Department for Communities and Local Government (CLG).

23. CLG are responsible for delivering the DfT(C)'s record management strategy in the following operational areas:

    - Communicating records management policy, including the Departmental Record Officer function
    - Providing registry services
    - Maintaining the records catalogue
    - Managing the file storage contract with Iron Mountain
    - Managing the archive review process
    - Providing deposited document services

24. In the DfT(C) the Information Management Directorate (IMD) has responsibility for a number of activities. These are:

    - IT platform for storing electronic documents
    - Security and Business Continuity
    - Information Rights Unit (FOI)
    - Strategy and Contact Services Unit, including management of Service Level Agreement (SLA) with CLG.
    - Data Handling Unit

25. IMD is currently developing a KIM strategy which will consider any appropriate changes to the above responsibilities.

PART THREE: ACTIVITIES CARRIED OUT BY THE ASSESSMENT TEAM

Methodology

26. The underlying purpose of the assessment is to establish whether the key elements of DfT'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.

27. DfT is divided into a number of key business 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 DfT business groups were split 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 raised by DfT themselves.

28. 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, sustainability of digital records

Access	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

29. 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

30. DfT 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

31. 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

32. 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

33. A review of DfT'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

34. 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

35. DfT's risk framework and associated information statements and policies were assessed to ensure information, knowledge and records management compliance.

Data Handling

36. DfT's data handling was reviewed in a limited context or "light touch" within the IMA process and only where there was an immediate effect on the process being reviewed.

The Assessment Team

37. 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, Doreen Charlton
   - Head of Standards, Marcia Jackson
   - Inspection & Information Management Consultant, Jeremy Harley

- Standards Adviser, Dan Husbands
- Standards Manager, John Williams

Assistance provided by the Department for Transport

38. The Assessment Team are grateful for the co-operation and assistance of all staff within the DfT(C), and especially the Strategy and Contact Services team for helping to facilitate the assessment.

PART FOUR: HIGHLIGHTS AND AREAS FOR IMPROVEMENT

Governance and Leadership

> "The DfT should provide effective leadership on Knowledge and Information Management capability across the Department."

39. DfT has recently begun considering the development of a knowledge and information management strategy. The strategy will detail the steps DfT will take to become a fully effective knowledge sharing and information exploiting organisation. This is to be commended. This assessment is seen by DfT as part of the process to inform the future KIM strategy.

40. The Permanent Secretary and the Director General Motoring and Freight Services have demonstrated a clear recognition of the need for strategic direction and this will aid the development of a KIM strategy and its final implementation. The strategy is currently being drafted by the Information Management Directorate (IMD) for approval by the management board in due course. In the interim DfT needs to assess how to raise awareness of good records and information management practice.

41. DfT recognises the importance of the data it holds and collects from its activities. This data is used to inform policy decisions from the setting of national speed limits to the regulation of key sectors such as bus and rail. In terms of information assurance and Freedom of Information (FOI) access, the value of the information is fully recognised and excellent progress has been made in developing an effective information assurance culture. However, a number of the areas visited by the team were not fully mature in terms of record management and the way information is shared between staff on a day-to-day basis - though the Assessment Team are aware of a number of areas of good practice in the DfT and the challenge for DfT is ensuring that good practice is spread across the Department. The definition of what constitutes information and its value to DfT(C) also needs to be further defined and disseminated.

42. Key Performance Indicators (KPIs) have recently been introduced on

Information Assurance (IA) to ensure that DfT(C) is performing effectively and delivering on its objectives. However, DfT is yet to set KPIs for knowledge and information management. The creation of KPIs to measure performance in this area would greatly increase DfT's ability to understand its performance and determine where current gaps exist.

Recommendation 1: The Department should develop a mechanism to measure its KIM performance. Guidance should be sought from the Government's Knowledge Council.

43. The Senior Information Risk Owner (SIRO) at Director General level has responsibility for the governance of information management in DfT, supported by the Director and a Deputy Director in Information Management Directorate. The SIRO provides management direction for records and information management in DfT(C), and takes a strong role, at Board level, in championing information management across the organisation. This role ensures that information management is seen as having a high priority, ensuring that information management implications connected to policy changes in ICT, security and risk management are considered in a timely and coordinated manner.

44. There may be a need to formalise this arrangement more clearly to ensure that the information assurance and information management agendas are seen to be joined up and co-ordinated.

Recommendation 2: The Department should formally identify a records and information management champion and strategic lead at Board level.

45. The Assessment Team are aware that an internal audit took place of DfT(C) records management in March 2008. As a result of the review, the Director for Information Management re-emphasised the role of the Business Records Officer (BRO) and its importance to the organisation in a letter to all departmental directors. This review is a good practice example of leadership engaging with improvements in information management.

46. A further review of record management in October 2008 identified some progress at the corporate leadership level; however the actual implementation of actions beyond this was unclear. The Assessment Team have subsequently been advised that the Deputy Director Information and Data Handling has reviewed the findings as part of the development of the knowledge and information strategy, and that the DfT Board has agreed a series of measures to improve the Department's records management performance.

47. DfT must ensure that IT and information management strategies are closely aligned as both areas of the business have a stake in the current electronic filing system, its future development and the potential impact on the business. If the IT and information management strategies are not aligned, the business benefits are unlikely to be fully realised. It is possible that technology will be applied without re-thinking the business requirements, processes and cultures. However, if the two strategies are fully integrated, a strategic approach to technology can contain costs and make the best use of scarce skills, ensuring flexibility for future business requirements.

Recommendation 3: The Department should closely align its IT and KIM strategies to ensure cohesion and consistency.

48. There is a good level of understanding at SCS[1] level of records and information management. DfT's focus on data security has led to increased awareness of information assurance and its impact on information management. However, although most managers are engaging with the concept of information management, a minority do not appear to be reinforcing or demonstrating good information management practice to their staff.

49. DfT would benefit from developing a similar and closely integrated reporting structure for information management as has been developed for information assurance. The direct line from asset

---

[1] Senior Civil Service

owners right up to Board level has led to an increased awareness of staff responsibilities. The same could be developed for information management. In conjunction with personal KIM objectives, and adequate training for all managers, this will lead to a higher rate of compliance.

Risk Register

50. Information risks are managed via an information risk register held by IMD. The risk register identifies and defines the potential information risks facing DfT. The corporate risk register also features information management related risks, one relating to the implementation of the Data Handling Review and the other to data loss. These risks are managed at management board level.

51. To fully assess the impact of information management on the business, the relevant corporate information management risks needs to be identified, assessed and mitigated. DFT has assessed the risks to security and data handling – it now needs to broaden the scope to include wider information management risks. Guidance on managing information risk in government departments is detailed in the document 'Managing Information Risk: A guide for Accounting Officers, Board members and Senior Information Risk Owners'.[2] This guidance should be used in assessing corporate information risks.

Recommendation 4: The Department should identify and assess information management risks across the board, including high risks on the corporate risk register as necessary.

---

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

Records Management

> "The DfT will ensure that our information is appropriately captured, described, managed and preserved and that the risks are controlled."

What to Keep

52. Traditional methods of record keeping have become increasingly challenged in the information-rich world of emails and other electronic media. Now, vast amounts of information are created by DfT on a daily basis. DfT(C) needs to be clearer about what information it should be keeping. The Department recognises the risks that exist of losing, of providing inadequate protection, or not being able to find critical information and the significant implications of this.

53. DfT(C) has devolved the decision on what information has business value to the individual, with some guidance from the Records Management Team within CLG. In a number of areas the team visited, this has resulted in inconsistency, with some users keeping everything and some keeping little on the formal records system. The DfT intends to mitigate this through its proposed records management strategy. The Department needs assurance that the right information has been captured to meet any challenge.

54. Without a well-considered and corporately-made decision on what information has business value, there is a risk that some parts of the organisation will not keep critical business information properly. Most notably, critical information may be lost which could result in negative reputational, legal or financial consequences. In addition, key policy decisions may be made without the critical information to hand, or new research may need to be undertaken at considerable cost.

55. Conversely, there is an additional risk that the Department could unnecessarily keep significant amounts of information with limited or no value. The consequences of this are an inability to locate critical information when it is needed and financial costs in locating and storing the information. Finally, there are also risks relating to the

protection of personal data if such information is kept unchecked beyond its lifespan.

56. DfT(C) has recognised the inherent risks of devolving the decision on what information to keep, and is now beginning a project to deliver a KIM strategy. This strategy is central to ensuring that DfT knows what it should be keeping.

57. It is essential that DfT's strategy on what information to keep is fully integrated with the KIM strategy and is informed by the records management community. If it is not successfully integrated, then the behaviours required for both strategies to be successful will not be implemented or embedded simultaneously. This may lead to confusion and misunderstanding amongst staff and will increase the risk of information mismanagement.

58. The development of the strategy is underway, however at this point it is anticipated that the decision of what to keep will be made at divisional level by the Heads of Division, with guidance from DfT(C). Heads of Division will ultimately be responsible for making the key decisions on what information has business value and should be retained.

59. Good central oversight and control over the process of deciding what information to keep is crucial. Whilst the process of devolving responsibility is necessary, there must be tight controls to ensure that everything that should be kept is kept. This must be controlled and managed in the same stringent way that DfT manages its own finances. If this process is not managed with central oversight, the risk will remain that critical information will not be captured.

60. In addition, there is a real need to ensure that those with expertise in information and records management within DfT and in the Records Services team at the Department for Communities and Local Government (CLG) are involved in the development of the new KIM strategy. The teams directly involved in the day-to-day business of managing information and records have a substantial amount of knowledge of this area. Their understanding of the business will

bring insight to the policy development process.

61. The development of this strategy will be the foundation and starting point for the improvement of record keeping and information management across the whole organisation. Once DfT has identified what information has business value, it will be better placed to decide how it should be captured, retained and either destroyed or finally preserved. DfT should therefore begin by deciding what to keep before developing the strategy on how that information should be managed.

62. The National Archives' project to support government departments in deciding strategically what information to keep, and for how long, is currently underway. The National Archives will work closely with the DfT(C) to assist in the development of this strategy.

Recommendation 5: The Department should assess what information has business value and should be kept. This guidance should then be disseminated to staff.

Recommendation 6: Records experts, including those in CLG, should contribute to the development of the new KIM strategy.

Recommendation 7: The Department should work closely with The National Archives in developing departmental policy on what to keep.

Service Level Agreement with CLG

63. When the 'Department for Transport, Local Government and Regions' split in 2002, a shared service was set up between DfT and DCLG to cover corporate functions such as HR, legal, IT and records management.

64. As the two departments have diverged, records management has been left as one of the few shared services still operating. CLG operates the shared service under a Service Level Agreement (SLA) with DfT.

65. The Assessment Team found that the contract was well managed and provided a good level of service, as prescribed. However, because DfT has not yet developed its own strategy on what information needs to be kept there is a risk that the service may not be delivering the best outcomes for DfT. Without the ability to oversee the qualitative aspects of records management there is no way for DfT to know if the information stored has business value, and whether business units are managing their key business information correctly.

66. There is a need for DfT to take ownership of its records management policy as it implements an effective KIM strategy. This will then better inform the relationship between CLG and DfT and ensure that DfT is able to articulate its business needs clearly and be assured that it is getting the best value from the contract.

67. This should allow for a shift in the focus, from a predominantly day-today provision of the service to the consideration of future service planning and policy development. The creation of the Information Rights and Data Handling Division may be the appropriate time to assess such a role. There is a risk otherwise that those who are most engaged with the process will not be able to contribute effectively to policy development.

Policy and Guidance

68. DfT currently has its records management policy and a considerable amount of guidance published on Transnet (DfT Intranet) for staff to use. The current guidance is limited to the use of the system and does not identify what information users should be keeping or retaining. This, coupled with the devolved nature of the decision making process, creates a disparity over what is being kept by DfT. The resulting risk is that critical information may not be captured.

69. Once a strategy to determine what should be kept corporately has been rolled out, there is a real need for DfT to directly own the information management policies and guidance and make them relevant to the strategy. The organisation can only decide how it will

manage its information once it has decided what information it is going to keep.

70. DfT has led from the front on implementing the Data Handling Review and established visible ownership and responsibility for information assets, and has improved handling of this sensitive information. It needs to do the same in identifying a senior lead on the handling of all sensitive and other information, to develop and champion the policies and guidance, and to report directly to the Board. The work in both these areas is inter-dependent and should be fully integrated to ensure consistency of message across the organisation. This will enable information to be valued, managed and protected through common and understood control mechanisms and guarantee that information management is given the necessary profile in DfT.

Recommendation 8: The Department should identify a lead on information management to champion the strategy on what to keep and ensure successful implementation of the future KIM strategy.

Approved File Plans

71. DfT implemented Approved File Plans (AFPs) across the entire organisation as a means of records storage in 2004. The AFPs operate usually at Divisional level and present a structure for storing and retaining information and records. The AFPs were created with the aim of providing consistency in the storage of information across the organisation and to allow some central control over corporate filing. The AFPs subsumed the Accredited Shared Drives (ASDs) that had been introduced in 2000 because these had not been widely adopted.

72. DfT has provided a 'container' or repository into which teams and individuals should file records. However, the Department needs stronger guidance as to what should be stored within them, clarifying what should be stored within the file plan, and using consistent definitions. If staff are uncertain about what they should be saving within the file plan, critical information might not be captured.

73. A number of respondents suggested that when material is stored in the AFP, the file structures are counter-intuitive and difficult to use to locate and retrieve information. This presents a further risk as time is unnecessarily wasted locating and sourcing information to re-use.

Recommendation 9: Once the Department has identified what information has business value, the Department should review if file plans are the most suitable means of capture for this information.

Email

74. The majority of DfT's business is conducted via email. Key policy decisions are made, disseminated and recorded in emails. Despite this, staff are unclear on what emails need to be kept.

75. To address this issue DfT should provide stronger guidance as to which emails should be kept as having business value, and which it is safe to delete.   Information contained in emails may have significant value to the business as they often provide an audit trail of policy and financial decisions.   When information with business value is identified by DfT, staff should be in a position to apply simple rules to identify what has corporate value and what does not.

76. There is a further issue of how to capture emails once they have been identified as having corporate value. The recent removal of a limit on email inboxes has left no incentive for users to store business-critical emails in any other repository other than their inbox. Most notably, the Assessment Team were informed that one user had 6,000 emails in their inbox. This is a risk as business critical emails forming part of an audit trail may not be captured as part of the formal record. Thus, they may not be available as evidence in an audit or judicial review.

77. The Assessment team have since been advised that DfT(C) have revised guidance on saving archived emails.

78. Under current arrangements, after sixty days in the inbox, emails are automatically transferred into an email archive where they are stored

indefinitely. The archive is fully accessible and retrieval of emails is reportedly a fairly efficient process. However, a number of interviewees reported that when emails are transferred from the email archive to an AFP, it is not possible for colleagues to access them. This presents a significant issue as key documents may be lost.

79. In addition, the indefinite storage of emails in a private personal archive presents an important concern, namely that this system is unsustainable. It will cost DfT a considerable amount to store these emails indefinitely with no inbox size limit.

80. Once DfT has identified what information should be kept, it should investigate alternative means of capture for email. This could, for example, involve electronic sweeps of inboxes with keyword identifiers. This would circumvent the need for users to file email in an alternative repository and would increase the likelihood of DfT capturing critical information.

Recommendation 10: The Department should review the risk of not having size limits on staff inboxes and investigate alternative means of capture for emails.

BRO network

81. DfT has implemented a Business Record Officer (BRO) network across DfT(C). This network includes a BRO in each team or division who discharges their BRO duties in addition to their substantive role. Most BROs interviewed estimated that BRO role took up approximately 10 per cent of their time.

82. BROs are, for the most part, graded at a junior level and therefore have limited authority in enforcing good records management practice. The majority of BROs' functions were limited to requesting the creation of both physical paper files and electronic files in the AFP. There was little evidence of BROs being involved in the wider records management area. In a small minority of cases BROs did have a part to play in training new starters on information and records management.

83. The BRO network would be more effective if its status and profile was increased. There would also be benefit in professionalising the work of the network and better integration of this role with other information management and publishing roles. The Government Knowledge Council is currently developing guidance on the professionalisation of KIM staff which should be of use to DfT[3]. In addition, the BRO network should become fully engaged with the development of a strategy on what to keep in order that they can become local champions and
ensure compliance. Local monitoring cannot be conducted without their support.

Recommendation 11: The Department should review the role of BRO to raise its profile and remit.

Recommendation 12: The Department should consider professionalising the role of BRO in conjunction with the guidance provided by the Government Knowledge Council.

84. A substantial proportion of staff interviewed as part of this assessment were unaware of the identity of the BRO in their team or division. In other cases, staff only approached their BRO if they wanted a file created, not to ask about other records or information management questions or queries.

85. When DfT has developed a strategy around what to keep, the BRO network will become invaluable in disseminating the corporate message and answering questions and queries at a local level. This will also prevent the central information management team becoming overloaded with queries.

86. The network is pivotal to DfT's intentions to increase information management awareness and good practice; it would be beneficial for DfT to demonstrate its commitment by actively managing the network.

---

[3] Guidance on Private Office Records-Cabinet office/The National Archives June 2009

Recommendation 13: The Department should take ownership of the BRO network to demonstrate its commitment to effective information management.

87. The Assessment Team were informed that the BRO network met through a series of BRO seminars arranged to meet an issue of demand. Beforehand BROs would be canvassed for items to be discussed. During seminars, presentations were given by members of Records Services on salient issues such as updates and guidance provided on aspects of records for the new IT platform, presentations by The National Archives and Iron Mountain. The last BRO seminar was held in November 2008.

88. It is recommended that BRO seminars are held on a more regular basis to create a sense of cohesion amongst BROs and allow problems and solutions to be shared across the organisation.

Recommendation 14: The Department should increase the frequency of BRO seminars and their scope to reinforce corporate information management messages across the network.

Retention

89. Records retention schedules identify the length of time a record should be retained by DfT before it should be reviewed and then either destroyed or preserved.

90. Other than among the BROs, there was generally limited awareness of the need to apply records retention schedules amongst DfT's staff. Most were unaware of the existence of such schedules and none of the staff interviewed had been asked to review records at any time.

91. All paper files have their retention managed from within the Records Management system, Livelink. This is a well established process.

92. Under current arrangements, it is the responsibility of the local BRO to log the creation of electronic files on the AFP with the CLG

Records Services team, and in doing so provide a retention period for the file. From the BROs interviewed, it appeared that for the most part a default five-year retention was applied. Where a retention period was identified it was stored on a database maintained by the CLG Records Services team.

93. The application of retention schedules to electronic documents is reliant upon the diligence of the individual BRO in logging the creation of the file with CLG. It is not clear how the retention is reviewed as the Assessment Team could find no evidence of any staff ever having reviewed a file in a formal retention/review process.

94. There is a risk that DfT may be retaining a considerable amount of information that it does not need to keep. This will incur significant costs for DfT in terms of storage. Similarly, DfT may not be keeping records for as long as it should (i.e. as long as they have business value), or not keeping them at all, when in fact they may have significant or long-term business value.

95. Until DfT has identified what information has business value, it cannot be confident that the retention periods applied to records are appropriate. DfT should therefore review its retention schedules after it has identified what information has business value. It should also look at different ways of applying retention which limit what the user has to actively do to apply them. For example, a user could simply identify a document as being in a particular category and a retention period would automatically be applied.

Recommendation 15: The Department should review its retention periods and investigate an automated process for their application.

Information Asset Register

96. An Information Asset Register (IAR) has been created to identify all the key information assets within DfT and allocate an owner to each. This process ensures that responsibility for each asset is clearly identified.

97. It was clear that all the Information Asset Owners (IAOs) interviewed were fully aware of their responsibilities for the register. They were all familiar with the quarterly reporting mechanism which includes a direct report to the Senior Information Risk Owner (SIRO) who in turn reports any risks to DfT's board and any data security breaches to the Cabinet Office via the Information Risk Return (IRR).

Data Security

98. Since the publication of the Hannigan Review of Data Handling Procedures in Government, and the publication of 'Managing Information Risk', Information Assurance (IA) and data security have become a priority for all government departments. The Department for Transport is no exception and has taken considerable steps to mitigate the risks to the organisation.

99. A number of interviewees reported that the Permanent Secretary had been instrumental in pushing forward the message on data security and had actively championed the new procedures put in place. DfT has led by example in this case and has ensured that all its staff are fully informed and are aware of the need for good information and data security.

100. The Cabinet Office Protecting Information mandatory e-learning module has been rolled out to all staff within DfT. All contractors' staff working for DfT and with departmental email accounts were also included, which is an example of good practice. In this case, DfT has very much led from the front and it was reported that all senior and middle managers had completed the online module. We understand that their remaining external contractors will be required to undertake the commercial version of the training now under development in 2010.

101. There was also a high awareness amongst interviewees of the importance of encrypted removable media. USB removable media was only used where there was a good business case for its use. All removable media is now encrypted as standard procedure.

102. Another example of good data security was the secure data room

maintained by the Procurement division. The secure data room allows sensitive information to be uploaded into a protected online storage area where third parties could gain access to it with a series of codes provided by DfT. This provides added protection and security.

103. However, there is still a risk relating to the storage of protectively marked material on the AFPs. Whilst in most cases it is possible to set permissions on folders within AFPs to protect the information contained within them, there were a number of examples cited where the IT department was unable to set adequate permissions. The reasons for this were unknown but appeared to be related to the limitations of the technology. This presents a significant risk as unauthorised access to data may be possible.

Recommendation 16: The Department should review the methods for protecting information held on AFPs to ensure that unauthorised access is not possible.

Private Office

104. Private Office currently uses the ministerial communication system (MinCom) to record all correspondence to and from the minister and this is stored electronically on the AFP. As MinCom contains personal data, there are stringent protections in place to prevent users gaining unauthorised access to the data without prior permission of the Information Asset Owner.

105. DfT needs to ensure that Private Office is clear on what information has business value. Otherwise there is a significant risk that potentially critical information may not be captured and retained. This could result in serious legal or reputational damage.

106. Since the Assessment Private Office have confirmed that they have liaised with the Departmental Records Officer to determine a course of action in relation to the storage of policy documentation under the Private Office guidance from Cabinet Office. After a process of consideration it was confirmed that policy units would continue to be made responsible for storing any documentation that is sent to or

from Private Office.

107. Private Office in DfT(C) follows Model Two from the Cabinet Office Guidance on Private Office Records.[4] This is acknowledged within the Guidance as the model that poses the most risk to an department. In a department that is not mature in how it manages its information across the board, there is potentially a serious risk faced by the department as the management of Private Office information is devolved to a large number of teams and individuals.

108. This system relies upon the Private Office being assured that the policy units are keeping a full and accurate record of all correspondence with the office. As DfT 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.

109. The Guidance recommends that the DRO undertakes an annual assessment of procedures within Private Offices. Private Office may wish to undertake such an assessment to provide assurance that the risks described above are mitigated. The Assessment Team recommends this course of action to provide evidence that the risks are mitigated and complete records are kept.

Recommendation 17: Private Offices to undertake an annual assessment of procedures to fully comply with Cabinet Office and The National Archives Guidance on Private Office records.

---

[4] http://www.nationalarchives.gov.uk/documents/popapersguidance2009.pdf

Access

> "The DfT will promote access to and re-use of our information, and protect personal and other sensitive information."

Data Protection

110. The implementation of the Data Handling Review has substantially increased awareness across DfT of the need to protect personal data that is held on DfT and its agencies' systems. All key dataset systems across the business are now registered on the Information Asset Register with an Information Asset Owner responsible for reporting to the SIRO on a quarterly basis. The Assessment Team is confident that all key datasets systems are appropriately protected.

111. The Data Protection team based in the central department, have contributed to the overall data handling policies for DfT and hold regular meetings with DfT's agencies to offer advice and consistency of approach on data protection.

Corporate Website

112. Although DfT has one central website (dft.gov.uk) it is also responsible for a number of 'campaign' websites which have a narrow policy focus and a public communication role.

113. While it is the responsibility of the policy units and publicity team to produce and maintain campaign websites the DfT web team is consulted during the development of campaign websites. Campaign websites are generally produced and hosted by third party private companies. In these cases Crown Copyright material is being stored on external systems over which DfT has limited or no control. There is a risk that key material may be lost because DfT is not able to exert adequate control over it. The DfT web team increasingly organise the hosting of campaign websites and is reviewing all external hosting arrangements as part of the service transformation work to look at the possibility of bringing hosting in-house.

114. DfT should also register these campaign websites with the Web

Continuity team at The National Archives to ensure that the websites are captured as part of the overall website capturing and archiving programme. This will ensure that an archived version is available for the public if these websites are removed and deleted by third parties.

115. The Assessment Team have subsequently been advised that all DfT campaign websites are now registered with The National Archives.

Recommendation 18: The Department should assess the risks relating to the hosting of DfT websites by third parties to ensure that they are managed effectively.

Recommendation 19: The Department should develop a policy round the creation of websites to ensure the DfT Web team are involved from the outset.

116. Similarly, there are concerns over DfT content appearing on external websites such as YouTube[5] and Twitter6[6]. The publication of third party owned video material on the YouTube website has possible implications for the infringement of intellectual property rights. This is something DfT needs to consider because it may be infringing copyright by publishing content over which it does not own intellectual property rights.

117. The Assessment Team have been advised that DfT are developing a social media policy to address some of these issues.

Recommendation 20: The Department should assess the risks relating to the publication of third party material on external websites in order to reassure DfT that it is not infringing intellectual property rights.

118. Twitter, a website that is being used to upload and publish 140-character messages is also being utilised by DfT. Ministers are

---

[5] www.youtube.com

[6] www.twitter.com

contributing to Twitter to share policy and to gain feedback from other Twitter users (i.e. the general public)[7]. Currently DfT is considering how best to capture this material so it can be retained for the formal record.

Recommendation 21: The Department should consider whether material produced on Twitter is critical to keep for the public and policy record and, if so, how it should be captured.

119. Based on extensive external research and user testing content on the department's website was categorised into Aviation, Rail, Road and Shipping modes. This can make it difficult for pan-transport policy and strategy topics to fit within the structure. These restrictions limit the ability of users to navigate easily around the site.

Recommendation 22: The Department should consider design improvements for their website to ensure joined-up content and interlinking between policy areas.

120. There are ongoing issues over content ownership on the corporate website. Content has effectively become orphaned in many areas due to lack of ownership. This is a risk because DfT may be displaying and communicating out of date information to the public. We understand DfT are undertaking an extensive content review to address these issues

121. As part of the DfT web continuity policy, the DfT web team ensures that copies of its own web pages are stored in The National Archives web archive before they are deleted from the DfT website. Any subsequent requests for that web page are then redirected to the archived copy which will remain accessible, allowing members of the public to access the information they are looking for without being confronted by a broken link. DfT has been an early adopter of the redirection component recommended by The National Archives.

---

[7] Guidance on a Twitter strategy for government:
http://www.scribd.com/doc/17313280/Template-Twitter-Strategy-for-Government-Departments

Recommendation 23: The Department should identify content owners for all material on the corporate website.

122. However, the website was still found to contain out of date and broken hyperlinks. The Assessment team were advised that it was not always possible to check which links on the site were broken due to the technological limitations of the current content Management system. Because of this users visiting the website may not be able to track down the information they are looking for because they cannot access a link. This will lead to a poor customer experience if it is not addressed.

123. The Assessment Team have subsequently been advised that DfT has purchased and regularly run software to automatically check for broken links.

124. The DfT Web team have been working closely with The National Archives' project on Web Continuity to capture a snapshot of the corporate website every four months and archive it. As part of this project there are plans underway to match up broken links on the corporate website with the archived content. This should ensure that users are able to retrieve the information they need quickly and easily.

Recommendation 24: The Department should ensure that it is adhering to the COI guidelines on 'Managing URLs' and 'Archiving Websites' to ensure compliance.

Re-use of Public Sector Information

125. DfT supports the re-use of its information and datasets and in conjunction with its publishers produces such publications as 'Know Your Road Signs'.

126. The Print Publishing Team, which is responsible for the re-use of DfT's information, has begun proactively seeking information and datasets from across the business to re-use.

127. This activity takes place in consultation with The National Archives which supports DfT in the provision of value-added licences. However, The National Archives will soon cease to provide value added licences for departments. It will therefore be necessary for DfT, if it wishes to continue to charge above the marginal cost, to apply to The National Archives for a limited delegation of authority.

Compliance

> "The DfT will make sure that internal processes support effective information management."

Protective Marking Scheme

128. There is limited awareness around what should be protectively marked and at what level (e.g. Protect, Restricted). A significant proportion of those interviewed appeared to be unsure or uncertain about the classifications and how they should be applied.

129. In a number of cases there appears to be a misunderstanding about how to apply a marking. In one notable case, a blanket protective marking was applied to all documents produced by one team. Even those documents not marked as protected were presumed to be protected merely by association.

130. In addition, the technological limitations of the AFP system mean that there is no prompt when documents are being saved to AFP to apply a protective marking. This means that staff are not reminded of the need to apply markings where in some cases they may be required.

Recommendation 25: The Department should investigate the possibility of a protective marking prompt when saving documents to reinforce good practice.

131. Similarly, if a document is protectively marked there is no flag on the electronic filing system to mark it as such. It is only once a user opens a document that they find whether it is protectively marked. This is a risk because it is not clear what documents are protectively marked until they are visible.

Recommendation 26: The Department should increase awareness of protective marking procedures through training and the provision of clear and usable guidance.

Recommendation 27: The classification of a document should be included in the document's title, so that it is visible to users. This could be achieved through an automated process.

Third-Party Contractors

132. DfT works with a number of contractors in various areas of its business. DfT has a mature approach to working with contractors which includes applying the same standards of information management that are applied to civil servants.

133. Contractors are given training on data handling, information assurance and records management through IT training packages and via their local BRO. In addition, contractors and civil servants work in mixed teams to ensure a consistency in working practices and engender an understanding of the importance of the formal public record. This approach should be commended.

Training

134. DfT does not run any corporate training in records and information management for general staff. In some areas of DfT, the local BRO provides training on records for new starters as part of the induction programme. This training is usually delivered at the desk of the new starter and includes instruction on the use of the AFPs and ASDs. There is, however, little in the way of training on what a user should keep and retain and what information has business value. This induction training is entirely dependent on the diligence of the local BRO in becoming involved in this process.

Recommendation 28: Information management training, in conjunction with information assurance, should be incorporated into the induction process.

Recommendation 29: The Department should assess the need for information management training to be included in information assurance training for general staff.

135. Conversely, DfT has successfully rolled out the Cabinet Office's e-learning module on data handling to all staff. The online module provides a basic overview of data handling procedures in government and is mandatory for all staff at all grades. This has played a significant role in increasing awareness around this area. A similar approach, integrated with ongoing information assurance activity, should be pursued for information management training.

136. Those staff in DfT with BRO responsibilities undertake initial training with the CLG Records Services team. This training comprises instruction on the creation of paper and electronic files, the AFPs and the recall of files from the offsite Iron Mountain archive.[8] As part of the BROs' ongoing training, they are invited to BRO seminars which are held when demand arises and consultation on the agenda.

137. Once DfT has developed a strategy which identifies what information it needs to keep, it should take ownership of the BRO network and utilise it to embed good practice across the organisation. If the BROs are fully informed and engaged with the strategy on what to keep they could act as champions and provide local training to staff.

138. The BRO seminars should also be used as an open forum for BROs to share and devise solutions to common problems and concerns. This would further engender a culture of knowledge sharing in DfT.

139. If DfT however does not engage with the BROs or make more use of the network, there is a risk that ineffective practices will continue to persist and the buy-in from general staff will be hard to achieve.

Intranet

140. 'Transnet' is DfT's intranet which is used for the dissemination of policies and guidance across the organisation, as well as acting as an up-to-date internal news channel for staff. Transnet is updated centrally by the Internal Communications team and by approximately twenty devolved editors.

---

[8] DCLG and DfT's offsite archive storage contract is held with Iron Mountain

141. DfT is currently planning a refresh of the intranet which will keep the same number of devolved editors, but will potentially add greater functionality to allow the sharing of information between users.

142. The Assessment Team were advised by a number of interviewees that content on the intranet is not always kept up to date. The Intranet team confirmed that they conduct a rolling programme of content reviews, but currently no formal process exists for the reviewing or updating of content other than on the Transport Story site. This is a concern because staff use the intranet to keep up to date with departmental activities and to check policies and guidance. If these are not kept up to date, staff will stop using the intranet and it may become an underused resource.

143. The Assessment Team have subsequently been advised that as part of the Transnet refresh the Intranet Team are developing a formal content lifecycle process which will include a six monthly review to ensure that content is kept up to date.

Recommendation 30: The Department should devise a process for reviewing intranet content to ensure that it is up to date.

144. DfT takes the view that the Intranet is a communication tool and not a records management system. Therefore, content on the intranet is not part of the public record. It is the responsibility of the policy owner to retain policy documentation, not the Intranet team. Some items such as Bulletin and Permanent Secretary Messages are archived, but other old content is not routinely archived. There is a risk in this case that although the content on the intranet may be considered ephemeral, some of the content may actually be part of the formal record and should be captured. Currently, once it has been removed from the intranet, it is lost. This must be considered to prevent the loss of business critical information.

Recommendation 31: The Department should review what other intranet content needs to be captured for the formal record to ensure critical business information is not lost.

145. DfT also operates a number of Localnets, on Transnet. These are used by teams, divisions or projects to publish and share team-specific information policies and guidance and some are managed by devolved editors. However, most are still managed by the Internal Communications team and all requests to add or change material on these Localnets have to go to through Internal Communications. Encouraging further devolved editors to manage Localnets may allow local teams to share information more easily.

Recommendation 32: The Department should review the number of Localnets to ensure that there is more local access to allow the easier dissemination of content and sharing of information.

Sustainability of digital records

146. The Department recognised the risks associated with digital continuity, such as the degradation of hardware, software, obsolescence, the loss of metadata which provides interpretation of key information and the loss of information during upgrades or restructures. If these risks are unmitigated there is an increasing likelihood that key critical information will either be lost or become unreadable.

147. DfT(C) contributed £110,000 to The National Archives Digital Continuity Project in 2007 and sought an update on the project in 2008. DfT(C) plans to act on the planned guidance and Framework tools and services that is anticipated in 2010.

Recommendation 33: The Department should undertake a digital continuity risk assessment within twelve months of the publication of this report in conjunction with The National Archives.

Culture

> "Information is recognised as the key asset for running the business of DfT and is used to support effective data and information sharing and knowledge creation."

148. DfT places significant value on the data it collects and uses for the purposes of policy making. It is clear that key policy decisions are based on evidence collected and analysed by DfT. It is therefore important that DfT manages this information effectively.

149. Although DfT has led firmly from the front on the recent implementation of the Data Handling Review, there is limited evidence of an awareness of effective information management. The recent appointment of a Deputy Director for Information and Data Handling, however, is a good first step towards creating an effective strategy in this area.

150. The Assessment Team found that whilst senior managers and practitioners generally understood the need for effective management of information, the middle-management level did not. At this level, many middle managers delegated all information management tasks to their staff and therefore failed to lead by example. Middle managers therefore need to be seen to be valuing and managing their information effectively to engender the same ethos in their staff. If this is not put into practice, staff will not engage with information management good practice. Under a new what to keep strategy, it is essential that middle managers engender the right attitudes in their staff.

Recommendation 34: The Department should develop a programme to increase awareness of effective information management amongst middle management.

Knowledge sharing and transfer

151. The staff intranet (Transnet) is quality controlled by the Internal Communications team. Other than devolved editors, staff contribute

to the intranet by submitting content to Internal Communications, who advise on layout and editing in accordance with good practice guidelines. There is scope for the redeveloped of Transnet to provide opportunities for more direct user input through, for example, moderated forums, to increase knowledge sharing and so reduce the risk of unnecessary work being undertaken when it may have previously been completed elsewhere.

152. The intranet and the Localnets are often not fully up to date with the most recent information. Similarly, the intranet is not equipped with a message board or forum for staff to post information on. This limits their ability to share knowledge on an immediate basis.

153. The Assessment Team were informed by a number of interviewees that there is little opportunity for cross-cutting work across the directorates. This also limits the ability of staff to share information and knowledge across the organisation. This creates a risk of a culture of knowledge hoarding where staff routinely keep information within their teams and vital knowledge is not disseminated effectively. Again, this can lead to duplication of effort and therefore unnecessary cost to DfT.

154. The majority of staff interviewed noted a lack of formal mechanisms for sharing and capturing knowledge within DfT. DfT does not operate an exit interview policy, with any such arrangements working in a local, ad hoc way. DfT would benefit from a standardised process whereby staff who left DfT would participate in a series of exit interviews to capture their knowledge. If such a programme is not undertaken DfT risks losing considerable knowledge as staff leave or move around the organisation.

155. Another government department, GCHQ, has developed a process to capture knowledge which could be used by DfT. Guidance on the model is available on the Government Knowledge Council website.[9]

---

[9] Available on: http://gkimn.nationalarchives.gov.uk/

Recommendation 35: The Department should develop a knowledge capture policy to ensure knowledge is not lost when staff leave the organisation.

Staff understanding of information risks

156. Staff understanding of information risks within DfT is generally limited. Whilst the risks around data handling are well understood, risks relating to the capture and use of information are less appreciated. Such risks include, for example, the incorrect destruction of critical information, the loss of, or inability to locate critical information, the lack of basic records-management discipline or the risk of technical obsolescence. These risks are rarely raised with staff.

157. Staff understanding of risk is better in some areas than in others. Most importantly, understanding of risks relating to Freedom of Information (FOI) requests are well understood across DfT. Similarly, the full-scale nomination of Information Asset Owners for each key information asset clearly demonstrates the understanding of some of the risks relating to information assets.

158. Many staff, however, continue to store key information on their personal drives, on their computer hard drive, in their email inbox or the email archive. This prevents access to potentially business-critical information in the individual's absence or if they leave the organisation. In addition, if the information is stored locally there is a possibility that the information may be lost if the hard drive becomes corrupt or damaged. The limited understanding of these risks indicates that there is still some way to go before DfT can be confident that staff fully understand the risks relating to poor information management.

Recommendation 36: The Department should develop a programme to raise awareness of the risks of poor information management, to reinforce and embed good practice.

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 and Leadership	1	The Department should develop a mechanism to measure its KIM performance. Guidance should be sought from the Government's Knowledge Council.
	2	The Department should formally identify a records and information management champion and strategic lead at Board level.
	3	The Department should closely align its IT and KIM strategies to ensure cohesion and consistency.
	4	The Department should identify and assess information management risks across the board, including high risks on the corporate risk register as necessary.
Records Management	5	Recommendation 5: The Department should assess what information has business value and should be kept. This guidance should then be disseminated to staff.
	6	Recommendation 6: Records experts, including those in CLG, should contribute to the development of the new KIM strategy.
	7	The Department should work closely with The National Archives in developing departmental policy on what to keep.
	8	The Department should identify a lead on information management to champion the strategy on what to keep and ensure successful implementation of the future KIM strategy.
	9	Once the Department has identified what information has business value, the Department should review if file plans are the most suitable means of capture for this information.
	10	The Department should review the risk of not having size limits on staff inboxes and investigate alternative means of capture for emails.

	11	The Department should review the role of BRO to raise its profile and remit.
	12	The Department should consider professionalising the role of BRO in conjunction with the guidance provided by the Government Knowledge Council.
	13	The Department should take ownership of the BRO network to demonstrate its commitment to effective information management.
	14	The Department should increase the frequency of BRO seminars and their scope to reinforce corporate information management messages across the network.
	15	The Department should review its retention periods and investigate an automated process for their application.
	16	The Department should review the methods for protecting information held on AFPs to ensure that unauthorised access is not possible.
	17	Private Offices to undertake an annual assessment of procedures to fully comply with Cabinet Office and The National Archives Guidance on Private Office records.
Access	18	The Department should assess the risks relating to the hosting of DfT websites by third parties to ensure that they are managed effectively.
	19	The Department should develop a policy round the creation of websites to ensure the DfT Web team are involved from the outset.
	20	The Department should assess the risks relating to the publication of third party material on external websites in order to reassure DfT that it is not infringing intellectual property rights.
	21	The Department should consider whether material produced on Twitter is critical to keep for the public and policy record and, if so, how it should be captured.
	22	The Department should consider design improvements for their website to ensure joined-up content and interlinking between policy areas.
	23	The Department should identify content owners for all material on the corporate website.
	24	The Department should ensure that it is adhering to the COI guidelines on 'Managing URLs' and 'Archiving Websites' to ensure compliance.
	25	The Department should investigate the possibility of a protective marking prompt when saving documents to reinforce good practice.

Compliance	26	The Department should increase awareness of protective marking procedures through training and the provision of clear and usable guidance.
	27	The classification of a document should be included in the document's title, so that it is visible to users. This could be achieved through an automated process.
	28	Information management training, in conjunction with information assurance, should be incorporated into the induction process.
	29	The Department should assess the need for information management training to be included in information assurance training for general staff.
	30	The Department should devise a process for reviewing intranet content to ensure that it is up to date.
	31	The Department should review what other intranet content needs to be captured for the formal record to ensure critical business information is not lost.
	32	The Department should review the number of Localnets to ensure that there is more local access to allow the easier dissemination of content and sharing of information.
	33	The Department should undertake a digital continuity risk assessment within twelve months of the publication of this report in conjunction with The National Archives.
	34	The Department should develop a programme to increase awareness of effective information management amongst middle management.
Culture	35	The Department should develop a knowledge capture policy to ensure knowledge is not lost when staff leave the organisation.
	36	The Department should develop a programme to raise awareness of the risks of poor information management, to reinforce and embed good practice.

APPENDIX TWO: GLOSSARY

AFP	Approved File Plan
ASD	Accredited Shared Drive
BRO	Business Record Officer
CLG	Department for Communities and Local Government
COI	The Central Office of Information
DfT	Department for Transport
FOI	Freedom of Information
GCHQ	Government Communications Headquarters
IA	Information Assurance
IAO	Information Asset Owner
IAR	Information Asset Register
IM	Information Management
IMA	Information Management Assessment
IMD	Information Management Directorate
IRR	Information Risk Return
KIM	Knowledge and Information Management
KPI	Key Performance Indicator
SCS	Senior Civil Service
SIRO	Senior Information Risk Owner
SLA	Service Level Agreement