CIVIL SERVICE

Information Management Assessment

Ministry of Defence
March 2009

The National Archives

Contents

PART ONE: EXECUTIVE SUMMARY

1. The Ministry of Defence (MOD) is a policy-making Department of State and the highest level military headquarters in the UK, providing political control of all military operations. The Department has an annual budget of around £35 billion and employs approximately 280,000 military and civilian personnel.

2. The MOD is a large and complex organisation undertaking operational, policy making, procurement, supply and support functions, all of which are underpinned by information. In addition, the MOD must account for its operations in theatre through operational records. The importance of these records cannot be underestimated and the need for them to be accurate, comprehensive and detailed is vital.

3. Information is unmistakably a key asset for the MOD and is valued throughout the department and the Armed Forces. The organisation clearly understands that the need to get the right information to the right people at the right time is paramount to effective and efficient operations. The published commitment from the Permanent Secretary and the Chief of the Defence Staff to the effective management of information, demonstrates the high priority assigned to information management within the MOD.

4. The key theme that has emerged from our findings is that the MOD has a core of committed information and records management professionals who are keen to deliver effective information management across the department. Through the creation of iHubs, the MOD has begun the process to standardise information management right across the Armed Forces and HQ. There is a clear understanding of the need to further develop maturity in relation to information management and this should be highly commended.

5. Air Command has developed its own IM Foundation Programme which is set to deliver a consistent standard of information management maturity across the entire Royal Air Force. Air Command's proactive approach in engaging with its staff on information management is a demonstration of the work to improve and standardise working practices.

6. However, despite the excellent progress made so far, more could still be done to raise the information management profile and to ensure that the potential risks to the department are mitigated. There is a real need for the good practice that is happening in various parts of the organisation to be shared with all teams. This would really assist in enabling standardised good practice to cascade down through the department.

7. The MOD should also take steps to ensure that adequate and relevant training is available for all civilian and military personnel. Currently, there is a substantial lack of relevant information management training for users, and where it does exist, it is over-subscribed.

8. Finally, the MOD should assess how it will ensure that records are retained for the appropriate period in the digital age. Historically, the MOD has had a comprehensive registry and administrative system in place, however this has changed with the move to electronic ways of working. Retention of records should be standardised across the organisation and applied consistently. In addition, the data migration strategy applied to the rollout of the Defence Information Infrastructure / Future (DII/F) is key to ensuring that the co-ordinated improvements in information systems continue, with the clear purpose of protecting its information assets.

9. The issues highlighted in this report and the recommendations made would take the MOD's information management capability to an improved level and address some of the challenges faced. We would encourage the MOD to implement these recommendations, with the support of The National Archives, in order to build on the strong capability already demonstrated.

PART TWO: INTRODUCTION

Information Management Assessments

10. 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.

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

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

12. The Permanent Secretary and the Chief of the Defence staff have declared their commitment to the IMA programme and requested that The National Archives undertake a focused IMA of the Department. The assessment provides the opportunity to examine the underlying administrative, policy and decision-making processes of the organisation to support good record and information management practices.

13. The IMA programme offers a range of assessment/verification activities including, a documentation review, focused audits on specific issue areas identified within a department and full on-site assessments of the core business areas/services.

14. The National Archives have been requested to review current methods of information storage and retrieval and file destruction policy across the Department as a result of the Rule 43 Letter issued by the Coroner in the Hercules XV179 Inquest. This report sets out the findings, conclusions and recommendations of The National Archives' focused IMA of the Ministry of Defence (MOD).

Ministry of Defence (MOD)

15. The Ministry of Defence is a Department of State and the United Kingdom's highest level military headquarters, providing political control of all military operations. The Department has control of resources for the Armed Forces of about £35 billion per year. Across the Ministry of Defence, approximately 280,000, military and civilian personnel work closely together to deliver Britain's defence. The Department is divided into separate Top Level Budget areas for

administrative purposes. It also operates nine separate trading funds/agencies and the Atomic Weapons Establishment.

16. The Ministry of Defence Head Office, located in London, is responsible under the direction of the Secretary of State for Defence and the Defence Council, the Defence Ministerial Committee, the Defence Board and the Defence Board for leading the Defence contribution to the development of the Government's foreign and security policy and wider Government objectives, and for translating those objectives into Defence policy and the Defence capability needed to deliver it. It is jointly run by the Vice Chief of the Defence Staff and the 2nd Permanent Secretary.

    The main functions of the Head Office are:

    Advising Government and accountability to Parliament

    • Advising Ministers (and other Government departments) on the development of the Defence contribution to Government policy;

    • Supporting Ministers and the Permanent Secretary (PUS) in discharging their Parliamentary accountability for Defence activities.

    Making policy and setting Defence strategy

    • Developing Defence policy and strategy, defining the military capability and other Defence objectives which meet the Government's policy aims and match the resources available for Defence;

    • Developing policy for the management of the Armed Forces in order to maximise their fighting effectiveness, efficiency and morale.

    Planning and resource allocation

    • Translating Defence objectives into a Defence programme through a framework of plans which set appropriate objectives and performance targets for Top Level Budgets, Process Owners and Senior Responsible Owners, matched to available resources.

Management of Defence

• Managing the delivery of planned objectives by monitoring the performance of Top Level Budgets, Trading Fund Agencies, Process Owners and Senior Responsible Owners against planned objectives, identifying and managing risks, and adjusting objectives and resources as required;

• Defining the corporate framework for Defence by setting pan-Defence policies and standards to ensure Defence meets legislative and other external requirements and continuously improves its business processes, and monitoring compliance and managing risks accordingly;

• Assurance that Defence systems for direction, internal control and management are effective.

Strategic direction of military operations

The Head Office's role in giving strategic direction of military operations includes:

• Providing briefing and decision support services to assist the Chief of the Defence Staff (CDS) in commanding UK military operations worldwide;

• Providing Ministers with military and politico-military advice on these operations;

• Ensuring that Defence is tied fully into all wider Government policy and decision making relating to these operations;

• Managing the media and communications context in which these operations take place;

• Maintaining the ability to manage crises, supporting Ministers, CDS and cross-Government mechanisms, and to present military and politico-military issues in an informed and analytical fashion – this requires Head Office to ensure a 24 hour capability to respond to events at the strategic level;

• Conducting near horizon planning (6 to 24 months), including contingency planning, concepts of operations and periodic strategic reviews, in coordination with wider Government;

• Contributing towards longer term Defence and wider Government planning.

RAF Air Command

17. RAF High Wycombe, situated at Naphill in Buckinghamshire, is the home of the Royal Air Force's HQ Air Command. It was formed on 1 April 2007, when the RAF's Personnel and Training Command and Strike Command merged. The creation of the single Command, with a single fully integrated Headquarters, equips the RAF to provide a coherent and coordinated single Air focus to the other Services, MOD Head Office, the Permanent Joint Headquarters and the rest of MOD[1].

Head Quarters Land Forces (HQLF)

18. HQ Land Forces controls about 80% of the troops in the British Isles and almost 100% of its fighting capability. HQLF's role is to deliver and sustain the Army's operational capability, whenever required throughout the world, and the Command comprises all operational troops in Great Britain, Germany, Nepal and Brunei, together with the Army Training Teams in Canada, Belize and Kenya.

19. HQLF has almost 75,000 trained Army personnel, the largest single Top Level Budget in Defence, with a budget of over £5.6 billion annually.

Information Management at the Ministry of Defence (MOD)

20. The Ministry of Defence creates, uses and stores a wealth of information which is core to its operation both at home and in Theatres of Operation. This includes information such as personnel records, financial records, estate management, operational records and performance information. The Chief Information Officer has overall responsibility for information, policy and records management in Ministry of Defence.

[1] http://www.raf.MoD.uk/organisation/rafcommand.cfm

21. The Ministry of Defence has published JSP 747 ‘Defence Information Management Policy’, in recognition that information in all its facets is a highly valuable resource for the organisation. Together with JSP 441 ‘The Defence Records Management Manual,’ this document, provides the core guidance that cover records and information management principles within the Department. These policies underpin all corporate and departmental information management activities with the aim of ensuring that knowledge, information and expertise within the organisation are utilised, preserved and developed for the future.

22. To assess the information management and records management processes and capability in the MOD, the Assessment Team reviewed core departmental documentation and interviewed a substantial number of staff from MOD Head Office, RAF Air Command and Head Quarters Land Forces. As this is a focused IMA, Fleet Command was not included in this assessment, but will be assessed when a full IMA of the Ministry of Defence is conducted in the future.

23. The Corporate Memory (CIO-CMem) team within MOD, has, for a number of years had its own internal programme of Information Management Assessments. To date, the Corporate Memory team have completed ten of these assessments, including Air Command and Permanent Joint Headquarters (PJHQ), and the Defence Science & Technology Laboratory (DSTL).

PART THREE: METHODOLOGY

24. The purpose of the assessment has been to establish whether the key elements of the Ministry of Defence's knowledge, information and records policy and protocols are effective in meeting the needs of Defence in the twenty-first century. In his inquest report relating to XV179, the Coroner for Wiltshire and Swindon made a number of recommendations in a Rule 43 letter issued to the MOD in October 2008. Recommendation A (v) stated that:

    "current methods of information storage and retrieval and file destruction policy are [to be] reviewed and documented."

25. The National Archives was subsequently asked to undertake a focused IMA of the MOD as a result of this recommendation. The purpose of the assessment was to provide a "snapshot" of the critical information management processes conducted by the business. The Assessment Team examined a range of standard processes, systems and documentation to determine its findings.

26. The Assessment Team assessed a sample of key services across both the corporate Ministry of Defence functions and the Armed Forces, including MOD Head Office, Air Command and Land Forces (HQLF). It was important to review, both the Service elements and the non-operational corporate sections of MOD, in order to assess the integrity of the systems and processes in place and also to support any conclusions made within the context of this report. The key business areas were considered according to a risk assessment carried out prior to the on-site visit. This was based on:

    a. the findings of the pre-assessment questionnaire;

    b. information management issues raised by the Ministry of Defence as a result of the Coroner's Rule 43 letter.

27. The assessment 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 resonance to the overarching requirements of the Rule 43 recommendation and the Department's commitment to improving knowledge and information management capabilities.

    a. 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
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

28. The Assessment Team:

    a. examined key policy and practice documentation relating to training, skills and processes;
    b. interviewed staff members from corporate HQ, the RAF and Land Forces;
    c. tested the processes used and reviewed their application at front line services.

29. These activities are described in more detail below.

Documentation review

30. The Ministry of Defence 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 records and

information. These interviews were used to determine how staff 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 overall procedural gaps. This included where appropriate records management systems, both paper and electronic, retention and disposal schedules, general guidance and working instructions.

The Assessment Team

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

    a. Doreen Charlton, Standards and Assessment Manager

    b. Marcia Jackson, Head of Standards

    c. Dan Husbands, Standards Adviser

    d. Andrew Dyer, Mandy Goldsmith and Siân Jones, Information Management Consultants

Date of Assessment

34. Visits to MOD Head Office, RAF High Wycombe, RAF Wittering, RAF Honington, RAF Northolt and HQ Land Forces, Wilton, took place between 16th February and 13th March 2009.

Assistance provided by the Ministry of Defence

35. The Assessment Team are grateful for the co-operation and assistance of all staff within the Ministry of Defence, and especially the staff within the Corporate Memory team for helping to facilitate the visit.

PART FOUR: HIGHLIGHTS AND AREAS FOR IMPROVEMENT

Governance and Leadership

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

36. The Ministry of Defence (MOD) is a large and complex department that has to balance the demands of providing core departmental functions with the conduct of military operations.

37. The public commitment from the Permanent Secretary and the Chief of the Defence Staff to manage the MOD's information in a manner that meets its operational challenges and its business objectives is a positive example of the priority that is assigned to information management. There is a clear commitment at the Defence Board level to manage information in an effective and coherent way. The MOD's request for The National Archives to provide an independent review of their processes is a clear demonstration of this commitment, which is highly commendable.

38. From the interviews undertaken by the Assessment Team, there is evidence of a strong functional reporting line on information management. In addition, corporate guidance on information and records management in protocols JSP 747 'Defence Information Management Policy' and JSP 441 'Defence Records Management Manual' provides evidence of the importance placed on good information management practices.

39. At the heart of information management is the Chief Information Officer (CIO) who is responsible for the Corporate Memory team (CIO-CMem). Information management is regularly discussed at the Information Dimension Steering Group chaired by the CIO. The CIO provides reports to the Defence Board on relevant information management issues for the Department.

40. Located within the CIO's directorate is the Departmental Records Officer (DRO), who reports to the CIO on records and information management policy. The DRO also chairs an Information Working Group, where information management policy, legislation, creation and implementation are discussed by information management practitioners. The Corporate Memory team are tasked with the creation/review and updating of JSP 441 and report directly to the DRO.

41. There is a real need for the CIO to have visibility and the authority to "champion" all aspects of records and information management at the senior level. In the current environment where data security and information integrity is paramount, the Department is not capitalising on the full potential of the CIO to drive through the needed changes in information management. The Defence Board needs an advocate to push corporate working and consistency for the benefit of the whole Department.

Recommendation 1: The role of the CIO to be reaffirmed to increase awareness of his role and his authority.

42. The Assessment Team have since been made aware of a study conducted into the role of the CIO between December 2008 and January 2009. The study was endorsed in February 2009 by the Permanent Secretary and the Chief of the Defence Staff. The CIO's new roles and responsibilities have now come into effect.

43. One of the major challenges faced by the MOD is the difficulty in establishing a corporate identity for the department, and with that, the authority to mandate corporate ways of working. There are a number of cases where policies developed in headquarters (MOD Head Office) were not promulgated down the Top Level Budgets (TLBs) and into the Armed Forces.

44. Although the Chief Information Officer's directorate is responsible for information management across the department, it was difficult for the Assessment Team to establish who exactly had the authority to enable the dissemination of the corporate MOD identity and ways of working. It was clear that the introduction, take up and dissemination of JSP 747 'Defence Information Management Policy' and associated protocols had not been consistently applied.

45. The inability to mandate what should be done and in what format it should be achieved, has the potential to dilute the effectiveness of the guidance and protocols already in place. From our interviews and from samples of local guidance provided, there were instances where the Armed Forces perceived that a local solution would be more appropriate or that corporate guidance was not mandatory.

46. The effective management of information with all the associated processes cannot be separated from the business of the Department in an ad hoc and a permissive manner. The Department must ensure that JSP 441 and JSP 747, and other associated guidance, is followed.

47. This can be achieved through the empowerment of the Corporate Memory team to act as the guardians of the information management processes. The Corporate Memory team already conduct an internal process audit programme to assess how well guidance and protocols are working. There is now a need for a robust programme to undertake a qualitative review of how information systems are used, with a reporting structure that allows an analysis of issues to be presented to the CIO and Defence Management Board on a regular basis.

Recommendation 2: The MOD to review the scope of the Corporate Memory team audit programme to raise the profile of the results within the department.

48. Contained within JSP 747 are a number of clearly defined roles pertaining to the management of information within the MOD. These roles are Senior Information Officer (SIO), Information Manager (IMgr), and Information Support Officer (ISO). Each role has varying levels of responsibility and authority for information management. The potential to embed good information management practice across the Department could be realised through the consistent application of these roles and assurance that they are effectively resourced across the MOD.

49. A wide level of understanding of information management would be an indicator of effective dissemination of JSP 747. The Assessment Team were informed that at MOD Head Office, there are regular IM Surgeries, attended by a number of Information Managers (IMgrs) and members of the Corporate Memory team. However, away from Whitehall, there was limited knowledge or attendance of IM surgeries and there is subsequently a risk that some areas within MOD could be unaware of relevant issues or developments relating to information management disseminated through this mechanism.

Recommendation 3: Corporate Memory team to review the membership and attendance of IMgrs at IM surgeries throughout the department, and to examine alternative ways of communicating good practice to IMgrs.

50. Prior to the publication of JSP 747, Air Command had developed and

implemented an Information Management Policy supported by an Information Management Maturity model. This is used to benchmark and plot progress of information management across Royal Air Force (RAF) stations. Much of the learning relating to information management within the RAF has been translated into JSP 747 for the Department.

51. The MOD recognises that effective information management should be based on supporting the critical business objectives of the department as a whole. The operational needs of the Armed Forces mean that this may be easier to achieve in tandem with an assessment of information as a risk.

52. The National Archives has produced guidance on 'Managing Information Risk' which may be beneficial for the MOD to review to ensure they are meeting their obligations in managing their information risks.

Recommendation 4: The MOD to identify, revisit and define information risk for the department.

53. The Assessment Team have since been informed that the MOD has now created an IM risk register which has been endorsed by the Defence Board.

54. Despite the progress made so far, more could be done to raise the information management profile and ensure that potential risks linked to ineffective procedures and controls within the Department are mitigated. The Assessment Team were unable to find evidence that information management was defined as a risk within the Air Command's risk register. The Assessment Team was informed that "elements" of information risk were only considered within other identified risks on the register.

55. There may be sound reasons for this, but it was not clear to the Assessment Team, at which level the decision was made to review information risk and assign the appropriate level of risk mitigation to it. As information and its management are integral to business, information management risks need to be clearly identified within Air Command.

Recommendation 5: Air Command to review the current level of information risk to the service.

56. The Assessment Team have since been informed that RAF Air Command has taken steps to define an IM risk and allocated a risk owner.

57. The Assessment Team, supported by the Corporate Memory team, sought to find examples of teams and individuals across the MOD who are delivering innovative and practical solutions, in order that these good practice initiatives are shared. Examples found included RAF Wittering, which has developed a macro (for electronic documents) that prompts users to name documents in accordance with the MOD naming convention. This alleviates the problem of not being able to quickly retrieve documents once they have been stored in the filing system.

58. Good practice occurring within pockets of the MOD should be communicated and shared right across the organisation. The pressure on time and resources mean that a mechanism for all staff to share initiatives such as the examples highlighted in this report would be highly effective.

Recommendation 6: The MOD should allocate ownership of responsibility for collation and publication of IM good practice initiatives.

Records Management

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

59. The MOD has made a considerable investment in ensuring that good records management practices are in place, and that they are supplemented by the appropriate infrastructure, in terms of technology, guidance and protocols. It is noted that the MOD presently does not have one complete document and records management system across the whole organisation. Instead, a variety of electronic and paper systems are in place, that attempt to mirror or standardise ways of working. Meridio is the MOD's electronic document and records management system (EDRM), but is currently only deployed to approximately seven thousand users in the department. The department also runs Windows NT File System (NTFS) environment and various other standalone systems.

60. As previously mentioned, the Corporate Memory team's programme of internal information management assessments provides the focus for comparing the MOD's own policy with practice. As an internal programme, it assists in building the expertise from within the organisation and communicates the corporate message across the Department. The Corporate Memory team take the recommendations from the IMA and produce an action plan to address the findings. To provide continuity and raise standards in the MOD, the Corporate Memory team continue to monitor the action plans until they are completed.

61. Being able to plot progress of the action plans also aids the Corporate Memory team in gaining an overview of the Department in order to provide the required support on information and records management.

62. To provide cohesion for the variety of systems in use, JSP 441, covers both the creation of paper and electronic records. It also contains details on both the legislation governing the management of records and the MOD paper filing protocols and archiving procedures. All staff within the MOD have access to JSP 441, via the MOD Intranet and Internet sites. The Assessment Team has been advised that JSP 441 is to be reissued in May 2009 following substantial revision.

63. There was widespread praise for the support provided by the Corporate Memory team, who are available if MOD staff have any queries relating to the JSP, file

plans or document control in general. The Electronic Records Management (ERM) team were also praised for their visibility and "hands on" approach. The ERM Team have played a major role in consulting and prescribing the mandatory top two levels of the official MOD file plan, in readiness for the full pan-MOD implementation of Defence Information Infrastructure Future DII(F).

64. The ERM team recently conducted a survey of uptake of the EDRM (Meridio) in November 2008 which demonstrated that it was under-utilised, and inconsistently applied. Most notably, 41% of respondents regarded Meridio as of negligible importance to aid them with their business or did not use it at all[2]. The Assessment Team are aware that the MOD have begun planning to address the outcomes from the survey.

65. As with all corporate policy, there is a need for clear standards and guidance to enable consistency across the entire organisation. For a department as diverse as the MOD, getting that balance is fundamental to engendering the required corporate standards in records management. The balance lies in ensuring that the enforcement of consistency does not hinder the effective day-to-day working of the organisation as there is a potential risk that this may stifle collaborative working and the effective sharing of information.

66. The Assessment Team found examples, in both Air Command and HQ Land Forces where corporate guidance has been translated into local work instructions that make JSP 441 accessible and less overwhelming for staff. In these instances, the effective translation of the corporate procedures was highly beneficial to the working practices at the local level.

67. The appropriate use of localising guidance can provide the means to embed corporate procedures. It is important that the guidance is reviewed periodically to ensure that it continues to be fit for purpose. The Corporate Memory team already undertakes an internal Information Management Assessment programme which could be used to monitor how JSP 441 is being applied and could also act as a conduit for good working practices to be disseminated across the MOD.

[2] Director General Information: Records Management User Survey 2008

Recommendation 7: Corporate Memory team to undertake a qualitative review of local guidance.

Retention

68. Although JSP 441 is a comprehensive document, more could be done to ensure that it is used effectively. For instance, amongst some users there was limited knowledge of which documents should be kept and how long they should be retained. The application of appropriate retention schedules was found to be non-existent or inconsistently applied across MOD Head Office, the RAF and the Army.

69. The need to articulate what the department should be keeping is paramount to the effective storage and retention of information with business value. The department needs to be explicit in its strategies regarding what information should be kept. The focus currently is on how information is kept, rather than what information should be kept.

70. The Assessment Team is aware that the Corporate Memory team are active in operational record keeping which is a good example of the principles of deciding what to keep. The MOD have begun engaging with The National Archives' "deciding what to keep" project, and are working towards exploiting ideas from around government. This will assist in embedding a culture within the department around deciding what to keep.

71. There were a number of instances reported where electronic records stored on the EDRM were automatically defaulted to a two-year retention period, without an assessment of the actual retention period required. The Assessment Team were also advised that since the implementation of the EDRM in MOD Head Office in 2004, all records within a particular team had been defaulted to five-year review and that to date, no records had been reviewed.

72. If this situation is not rectified across the MOD, there is a risk that this will eventually put pressure on the department's resources to conduct the review. In the face of external pressures, a coordinated and timely review of records needs to occur for this to be effective. Retaining information beyond its need could also potentially expose the MOD to risks under the Data Protection Act.

Recommendation 8: The MOD to review and monitor adherence to the retention policy.

73. For the MOD, a fundamental part of records management is Operational Record Keeping (ORK). Operational records are responsible for documenting the main aspects of operational activities in theatre. All operational records are required to be collated and completed by the end of each month. The RAF and the Army have different systems in place.

74. In the Army, all operational records (Form 2118) are sent in electronic format to the Historical Analysis Team (part of the Corporate Memory team) at MOD Head Office. These are then checked and collated by the team. As a further improvement, periodic sampling of the content should be included in the process to ensure consistent quality of the operational records and the future integrity of the information. This sampling could then be used to inform the scope of future pre-deployment training. Information that is not received within the month are followed up by the Corporate Memory team. The Assessment Team recommend that the Historical Analysis team conduct a sample qualitative review of the records periodically to assess the information contained is of the required standard.

Recommendation 9: The Historical Analysis team consider the application of a qualitative review of a sample of the received operational records.

75. The Army's operational records are managed and held on separate standalone systems as they cannot currently be stored on the corporate EDRM on the Defence Information Infrastructure (DII) system. The systems are configured and managed by the team. The Historical Analysis team are able to access and retrieve this information as required. This system appears to be working well and the Corporate Memory team are confident that they are well placed to meet future demands on the service.

76. The main area of concern and a potential risk for the MOD is that as the operational records have to be held on separate standalone systems which are not supported by the MOD IT support, all the technical expertise relating to the maintenance and structure of the system is invested within the team. There does not appear to be any succession planning to cover the specialist technical knowledge that the team have acquired, should the need arise.

77. Data held on systems or servers that are not supported centrally is at high risk of becoming incomplete, unavailable or unusable. This would be principally through lack of support, loss of knowledge in maintaining the servers or systems, corruption or obsolescence. In time The National Archives' Digital Continuity Project will provide guidance on managing data or managing the transfer of data to supported systems.

Recommendation 10: Corporate Memory Team develop a succession plan to cover the technical skills within the Historical Analysis team.

78. In contrast, all operational records (Form F540) within the RAF are managed by the Air Historical Branch (AHB) based at RAF Northolt. AHB have produced a comprehensive guide on the completion of the F540, which contains guidance on what information should be included and provides examples of previously completed F540s under the heading "The Good, The Bad and The Ugly". This is an aid to the qualitative management of the operational records.

79. It is estimated that monthly the AHB should receive up to 120 separate F540s, but it was noted that these were not always received in a timely manner. It was also noted that on occasion the AHB were unable to chase missing or incomplete forms until a period of three to six months had elapsed. The longer the delay in collating the information, the higher the risk that potentially important information is not recorded in the operational record. This may pose a risk to the quality and usefulness of the operational records to the RAF and the MOD in the future.

Recommendation 11: Air Command reinforces the importance of completing the F540 within the month.

Recommendation 12: AHB develop an escalation process for non-receipt of F540s.

80. All operational records held by AHB are in paper format. If the F540s are produced electronically, they are printed by the Squadron (or similar) before being sent to AHB. Although this may meet the needs of the RAF at present, the global move to electronic records and information management may solicit the need to review the paper format to find a more appropriate format in the long term.

Recommendation 13: AHB assess the future viability of receiving and storing the F540 in an electronic format.

Handover

81. Across the areas assessed, there appears to be a shortfall in the potential exploitation of previous knowledge and information held by individuals and teams at the time of handover between exiting and incoming postholders. The MOD is one of a number of government departments where large numbers of personnel regularly change roles and duties over a two to three year cycle. Retaining this knowledge is important in ensuring that the department maximises the information flow and information sharing effectively.

82. The information or records created by the current postholder are not always readily accessible to his or her successor. There were several reasons cited for this, including time pressures, posts being gapped (i.e. not filled immediately), changes in business needs or organisational changes. HQLF provide local instructions that set out what needs to happen to ensure that business emails and files are ready for the next postholder. The application on how well this was applied was not tested. The RAF also had an example of a considered handover, which included extensive notes and links to the file plan. However, these examples were the exception rather than the rule across the areas assessed.

83. The culmination of poor handover information or 'gapped' posts gave rise to a reluctance to search for information held in inherited folders and files. There was evidence of staff copying files onto disks and then deleting the information without reviewing what was held. There is the potential risk in these cases where critical information could be lost to the organisation.

Recommendation 14: The MOD to review the application of handover procedures as part of its IM activities.

84. There was the perception across the areas assessed, that standards relating to the effective management of records within the MOD had declined, the loss of specialist registry/administrative posts being cited as a reason for this. A number of interviewees believed that the discipline around the management of registered paper files still existed, but that it needed to be translated to meet the electronic record keeping environment.

85. The continuing existence of specialist registry staff is acknowledged by the MOD to be neither appropriate nor feasible in the long term, as the majority of communication and work processes are via electronic methods. The MOD has had to change culturally to accommodate the new working environment and has redefined resources and operational priorities to meet these new challenges. As skills are redeveloped and new staff are recruited, there is a potential risk that a less disciplined records management approach, if not addressed, may adversely affect how records and information are managed in the future.

86. There are also positive examples within the MOD where the organisation has addressed the changing work environment and reviewed the skills needed to meet business requirements. Across both the RAF and the Army there was evidence that former registry staff had been absorbed into roles that included traditional registry elements, but for the electronic age. In the RAF there were also examples of former registry staff being responsible for the filing of all electronic documents via the iHub. In HQLF, the majority of iHub staff had formerly been the SPS registry clerks.

87. Staffing of the iHubs is left to the individual services to adopt an approach that meets their business objectives. Being able to retrain and retain existing skills within the services allows for levels of continuity in effective records management.

Archiving

88. The MOD needs to ensure a cohesive approach to handle the information that is currently held on redundant or soon to be redundant IT legacy systems. An illustration of this is the 'Corporate HQ Office Technology System' (CHOTS), still in use in some parts of the MOD in the UK and overseas. Staff raised concerns about how the information held on CHOTS would be archived or disposed of, as and when migration to DII(F) occurs. There is a risk that the information held is not destroyed or migrated at the appropriate time.

89. To maximise the potential for retrieving and retaining relevant information and records, there needs to be a co-ordinated approach to mapping the information that is held and a decision made to destroy what is no longer required. This will both free up resources needed to maintain the system, and also lessen the risk

that information is held needlessly.

90. The Assessment Team has subsequently been informed that, as part of the roll out of the Defence Information Infrastructure / F programme, there is a comprehensive data migration strategy whereby data on legacy systems is migrated either to a Windows New Technology File System or ongoing access provided via a reach back facility. For systems where data is not due to be migrated, there is a separate programme to ensure appropriate management of the data.

Recommendation 15: The MOD to review the risks relating to incomplete or inconsistent migration of data from legacy systems to DII/F.

Compliance

"I will make sure that our internal processes support effective information management."

Policy and Guidance

91. MOD has, within the last couple of years, issued or re-issued two Joint Service Publications on information and records management. JSP 441 'Defence Records Management Manual' and JSP 747 'Defence Information Management Policy' have been issued by the Chief Information Officer and serve to provide detail on information management protocols and the management of paper and electronic records.

92. Whilst both JSP 441 and JSP 747 contain all the necessary guidance for the conduct of information management, they are considered by some MOD staff to be overwhelming and too dense to find the information needed quickly. Some teams have adopted the practice of simplifying the guidance and producing crib and summary sheets to summarise the key information on a particular topic for the purposes of accessibility and understanding.

Recommendation 16: The MOD to review relevant information management policies for coherence and usability.

93. Air Command has developed its own five-part Information Management Policy. The document is highly comprehensive and contains a substantial amount of information, but is not easily accessible to the average user because of the amount of information contained within the guidance. There is a risk that because this guidance is not easily accessible, it will not be widely understood and it will not be cascaded down the chain of command to the relevant users.

Recommendation 17: Air Command to review its IM policy to produce accessible summary guidance notes, consistent with corporate policy.

94. Contained within JSP 747, is the MOD's model for how information should be managed within the department. The key principles and requirements of a "model" of IM management is the creation of an Information Hub (iHub) structure. It is expected that all services and core businesses set up or are affiliated to a local iHub.

95. iHubs ('Information Hubs') have now been rolled out over much of the MOD to replace the function of the traditional registry. Most iHubs are in their infancy; however a few are now well established, such as the iHub at RAF High Wycombe. A number of iHubs have inherited some of their previous registry functions, such as making travel bookings which has meant a diversion from the intended information and records focus. There also appeared to be uncertainty in some iHubs as to their primary role and their place in the iHub structure.

96. Senior Information Officers (SIO) are appointed at every RAF station and have responsibility for reporting on information management to the Station Commander. Information Managers (IMgrs) and Information Support Officers (ISO) are appointed further down the chain of command.

Recommendation 18: The MOD to continue the rollout of iHubs, with an emphasis on clarity and communication of role, whilst also supporting the existing iHub structure.

97. Subsequent to the assessment, the team were informed that the MOD has defined the purpose of the iHub in IM Protocol 015, last re-issued on 13th March 2009.

98. The RAF IM Foundation Programme is currently being rolled out to all forty-one RAF stations. The programme is working to bring all stations up to a consistent information management maturity level across the RAF. With a clear lead from Air Command, stations are required to ensure that their information management capability is meeting the required standard defined in the IM Foundation Programme. A campaign plan has also been developed to ensure that the programme is effective across the RAF.

99. As part of the RAF IM Foundation Programme, Air Command has introduced specialist software to identify excessively large files, duplicate files, and incorrectly filed documents in the file plan. This is a good example of the RAF's

proactive approach to cleansing its file plan and ensuring that data is not being stored in duplicate or unnecessarily. It is also good preparation for the introduction of the DII (F) system which will limit storage capacity for each user.

100. Air Command is currently rolling out a file plan structure to all of the RAF stations. Whilst the two top levels are mandated, each station can create a further four subsequent levels in the file plan to fit with their station's structure and activities. The corporate file plan will greatly assist with creating a commonality between each station.

101. The Assessment Team was shown file naming macros used in some RAF stations to ensure that emails and documents were given titles conforming to MOD naming conventions. This allows for a greater chance of retrieving the document or email once it has been stored in the file plan.

Recommendation 19: Assess the feasibility of introducing a file naming macro across the MOD.

Training

102. The MOD delivers all corporate training for Senior Information Officers (SIO), Information Managers (IMgrs) and Information Support Officers (ISO) at the Defence Academy. Although the courses are not mandatory for personnel in those positions, staff are encouraged to attend. The one-week and two-week Information Managers courses are held frequently and are reportedly well over-subscribed on every occasion. HQLF are heavily involved in the structuring and content of the ISO course which covers subjects such as "The IM key roles and the iHub" and JSP 441. Since the training began three years ago, the number of attendees on the IM courses has totalled 427[3] across all the Top Level Budgets.

103. The Assessment Team found evidence that some staff had chosen not to attend a course at the Defence Academy because it was too time consuming and would stretch resources within their team. Others, who had chosen to undertake the training, including some SIOs, had not had an opportunity to attend until well into their posting. This was either because it didn't fit easily into their schedule or because they were unable to get a place on a course.

[3] Figure supplied by the MoD on 17/03/09

104. The Assessment Team has subsequently been informed that a review has taken place to determine training needs across the department. From September 2009, the department will offer an increased IM course capacity. It is recommended that IM training provision continues to be reviewed and monitored to ensure training is available to all staff who require it.

Recommendation 20: The MOD to assess provision of IM training for SIOs, IMgrs and ISOs.

105. Training in information management for MOD staff and personnel not assigned to a specific information management role, was limited. Most staff, when asked about training, recalled training in the use of their IT systems but not specifically related to information management. MOD's IT contractor is responsible for delivering training specific to the DII system and older NTFS system. This training is IT focused and therefore concentrates on how the system works rather than the day-to-day practicalities of records management. The Corporate Memory team does not have a direct influence over the content or coverage of the training.

106. The Corporate Memory team does however deliver focused and ad hoc training and briefings when required, for example on the document disposal and retention schedules for PJHQ in 2007. As the Corporate Memory team interact with users on a daily basis it would seem appropriate that the team has a direct input into the information management training that is delivered for all IM and all non-IM specific roles.

107. The MOD would benefit from training all staff in information management practices, therefore familiarising staff with the appropriate policies and guidance as set by the CIO organisation. This would ensure a greater understanding of the value of information and the need to store and retain it appropriately.

Recommendation 21: The MOD to assess information and records management training needs for all staff.

Recommendation 22: The Corporate Memory team becomes formally involved in the process of devising and delivering IM training to all MOD staff and personnel.

108. Operational Record Keeping (ORK) training is inconsistent across the Armed Forces. Whilst the Army provides training in ORK during the pre-deployment training cycle for all personnel, the RAF does not provide any training unless requested. As operational records are a vital record of the MOD's military operations and subsequently provide essential information and evidence for potential subsequent inquiries, it is imperative that a full and accurate record is kept.

Recommendation 23: Training on Operational Record Keeping be included in all Pre-Deployment Training.

Culture

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

109. Historically, the Ministry of Defence has understood that operations in theatre would not be effective without good information management. The public commitment of the Permanent Secretary and the Chief of the Defence Staff has raised the profile of information management and given credence to high standards of IM within the MOD.

110. The role of the Defence Board is pivotal in getting the right message across, above and beyond that which can be gleaned in the numerous JSP documents within the Department. This joint approach is fundamental in adopting a holistic approach to a functional information management policy that takes into account people, processes and technology, all of which are interdependent. The challenge now is to promulgate "what IM means for the MOD" to all civil servants and military personnel so they understand what is expected of them, organisationally and professionally.

111. It was highlighted to the Assessment team that the majority of senior management discussion regarding information management, is about technology and systems. The perception was that systems were seen as the panacea to meeting the knowledge and information challenges faced presently and in the future. The investment in Defence Information Infrastructure Future (DII (F)) and the plan to roll it out to approximately 300,000 users in the next five years is a huge commitment at an estimated cost of £4.9 billion.

112. Concern was raised regarding the level of visibility of information and records management below the Defence Board level. Despite the CIO having responsibility for both records and information management, it was noted by interviewees that although records management and information management are related, they are separate entities, which are not integrated. Despite the best efforts, JSPs 441 and 747 add to the confusion.

113. This lack of clarity gives out a disjointed message. To challenge this, the CIO and his directorate must take and demonstrate a co-ordinated approach to

records management and information management across the department and ensure that this is filtered across the MOD.

114. Within both the RAF and the Army, information in its traditional sense is to support operations in theatre. The potential benefits of effective records and information management is recognised and established, mainly because it cannot be separated from their overall purpose. To support this commitment, the team met several staff who had already or were about to study for an MSc in Information Management at the Defence Academy. However, a relevant records or information management qualification was not consistent across the MOD. There was evidence that areas within the MOD that had knowledgeable qualified staff were able to enthuse other staff and colleagues and keep managers committed locally to the importance of good information management and record keeping.

115. IM Surgeries are held in head office, but only a minority of staff had either attended or been aware of its existence. The MOD should harness that enthusiasm and the skills of these officers to support the Corporate Memory team, with more regular forums to air these concerns and keep the front line information management practitioners supported.

116. Both the RAF and the Army have localised what information management means for their service area, and although good in some respects, there is a tendency to dilute what the MOD as an organisation needs to do. MOD Head Office must position itself to review/sanction a sample of the local processes to ensure compliance with the relevant JSPs.

117. The creation of specific information management roles within the MOD is welcomed. The requirement that all areas of the business manage information through the creation of local iHubs is a great innovation. Where iHubs are established they provide a core of expertise and reference point for their individual teams, stations and groups.

118. The set up of iHubs are reasonably flexible to reflect the priority needs of where they are located. The services provided varied from a ‘one stop service’ for filing electronic and registered files, management of the file plan, providing local station specific guidance on good record management and practice, and to provide support and update the material for individual Intranet sites.

119. The flexibility of purpose for the iHub creates a different set of issues that need to be addressed. As the iHubs are asked to perform differing roles, the time allocated to staff to champion information management varied considerably, with estimates varying from 10-50% of time. The current iHub staff are a combination of military communication specialists, IT professionals and administrative personnel.

120. As these roles have additional responsibilities, the team uncovered conflicts with main duties, in particular, when there were pressures on resources, due to gapped posts or operational needs. This has naturally led to a loss of momentum in pushing information management forward. Some interviewees acknowledged that the coroner's recommendation and the IMA undertaken by The National Archives had galvanised areas to progress the information management agenda.

121. The knowledge and understanding of information management by the senior and middle management also affected how an iHub was created and used locally. Those stations that had consistent leadership and actively promoted good information and records management principles, performed the best. These also happened to be the areas that had strong links with the Corporate Memory team in MOD Head Office and actively participated in projects and gave feedback. This level of leadership needs to be consistent across the piece, and the successes celebrated.

Recommendation 24: The MOD to develop an information management training seminar or briefing specifically for Managers.

Performance Management

122. The ability to use statistical information to support the records and information management agenda had a number of challenges to overcome. Where performance information was produced locally it was used by management in a variety of ways both formally and informally. In some RAF stations, local statistics were provided by the iHub or technical staff, to monitor use of electronic systems. For example, to monitor the size of email mailboxes so that individuals were encouraged to review the information, store business critical information or destroy irrelevant material.

123. Local reports were also used to encourage the use of the EDRM, and to identify teams or individuals who had failed to file items. Where there were peaks and troughs in filing records to the EDRM this led to a review of Teamsites (on Sharepoint) to assess what length of time documents were held in the shared area prior to filing. The local performance statistics enabled teams to review resources and also acted as a catalyst to enquiring if there were factors that inhibited their use.

124. The local performance solution was developed as a direct consequence of being unable to get official statistical information via the corporate IT contractors. The Assessment Team were advised by several interviewees that on a number of occasions, information that was agreed to be sent periodically by the IT contractors would not arrive, or was several days late. Data requested included information on the amount of storage used on team/station drives.

125. The Assessment Team were unable to assess contributing factors for the causes of this as this was outside the scope of the IMA.

126. There does not appear to be a mandatory statistical framework in place to support information management within the MOD. This information, if more widely available, could potentially add value as a tool to ensure systems are being used in an efficient and effective manner. The availability of this information would also be of benefit to the ERM team, who would be able to assess periodically how and where systems were being used, as part of an ongoing qualitative/audit function.

Recommendation 25: The MOD to review the existing performance reporting framework and assess the deployment of reporting tools for information management.

127. It is impossible to conduct an assessment of records and information management in the MOD, without acknowledging the impact of the IT systems and infrastructure. The Department does not have an organisational-wide single operating system. Instead, there is a wealth of differing and sometimes conflicting systems. Throughout the on-site assessment the limitations relating to the type, age and interoperability of the various IT systems across the organisation was evidenced.

128. Many of the IT systems within the MOD are specialist and for a number of reasons, including security, it is not feasible or possible to have a comprehensive fully integrated IT system. Where this is feasible, core parts of the Department are supported by an EDRMS and the latest version of the Defence Information Infrastructure. These have an improved interface with other systems that enable greater information sharing and collaborative working. In contrast there are some parts of the RAF still using NTFS based operating systems that are over 15 years old. Additionally, numerous standalone applications and servers are managed locally.

129. For the older systems, long term concerns that the MOD has started to address are the need for continuing support for the ageing parts of the network and managing obsolescence, as the manufacturers withdraw support for elderly operating systems. These are being addressed through the roll out of DII(F) across the whole of the MOD by 2014. The reality is that this has impacted on how records and information management has developed across the MOD.

The Future/Change Management

130. Changing the behaviours and establishing authority and the rights to mandate are steps in the right direction. Until that point, designing and promoting guidance that is relevant and accepted by all areas of the MOD needs to be a priority for the Chief Information Officer's Directorate. The Corporate Memory team are already developing a mandatory top level corporate file plan, similar in structure to that being implemented across the RAF. This has the potential to further embed uniformity within the MOD.

131. To further develop the potential of the file plan in readiness for DII(F), the Corporate Memory team should co-ordinate and provide guidance in piloting the use of the data mining software capabilities, identified in the RAF, in tandem with developing the corporate file structure to ease the migration of records to DII(F) by 2014.

Recommendation 26: The MOD to explore the provision of information management software tools to assist in the preparation for DII/F and longer term information management.

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	The role of the CIO to be reaffirmed to increase awareness of his role and his authority.
	2	The MOD to review the scope of the Corporate Memory team audit programme to raise the profile of the results within the department.
	3	Corporate Memory team to review the membership and attendance of IMgrs at IM surgeries throughout the department, and to examine alternative ways of communicating good practice to IMgrs.
	4	The MOD to identify, revisit and define information risk for the department.
	5	Air Command to review the current level of information risk to the service.
	6	The MOD should allocate ownership of responsibility for collation and publication of IM good practice initiatives.
Records Management	7	Corporate Memory team to undertake a qualitative review of local guidance.
	8	The MOD to review and monitor adherence to the retention policy.

	9	The Historical Analysis team consider the application of a qualitative review of a sample of the received operational records.
	10	Corporate Memory Team develop a succession plan to cover the technical skills within the Historical Analysis team.
	11	Air Command reinforces the importance of completing the F540 within the month.
	12	AHB develop an escalation process for non-receipt of F540s.
	13	AHB assess the future viability of receiving and storing the F540 in an electronic format.
	14	The MOD to review the application of handover procedures as part of its IM activities.
	15	The MOD to review the risks relating to incomplete or inconsistent migration of data from legacy systems to DII/F.
Compliance	16	The MOD to review relevant information management policies for coherence and usability.
	17	Air Command to review its IM policy to produce accessible summary guidance notes, consistent with corporate policy.
	18	The MOD to continue the rollout of iHubs, with an emphasis on clarity and communication of role, whilst also supporting the existing iHub structure.
	19	Assess the feasibility of introducing a file naming macro across the MOD.
	20	The MOD to assess provision of IM training for SIOs, IMgrs and ISOs.
	21	The MOD to assess information and records management training needs for all staff.

	22	The Corporate Memory team becomes formally involved in the process of devising and delivering IM training to all MOD staff and personnel.
Culture	23	Training on Operational Record Keeping be included in all Pre-Deployment Training.
	24	The MOD to develop an information management training seminar or briefing specifically for Managers.
	25	The MOD to review the existing performance reporting framework and assess the deployment of reporting tools for information management.
	26	The MOD to explore the provision of information management software tools to assist in the preparation for DII/F and longer term information management.

APPENDIX TWO: GLOSSARY

AHB	Air Historical Branch
CHOTS	Corporate HQ Office Technology System
CIO	Chief Information Officer
DII	Defence Information Infrastructure
DRO	Departmental Records Officer
DSTL	Defence Science and Technology Laboratory
EDRM	Electronic Documents and Records Management System
HQLF	Headquarters Land Forces
IMA	Information Management Assessment
IMgr	Information Manager
ISO	Information Support Officer
JSP	Joint Service Publication
MOD	Ministry of Defence
NTFS	Windows NT File System
ORK	Operational Record Keeping
PJHQ	Permanent Joint Headquarters
RAF	Royal Air Force
SIO	Senior Information Officer
TLB	Top Level Budget