The National Archives

Information Management Assessment

Ministry of Defence

Reviewed

February 2017

Published

November 2017

Working with government
to raise standards in information management

Contents

Statement of commitment

Before each Information Management Assessment (IMA) we recommend that a statement of commitment to the assessment process is published. The following statement from the Permanent Secretary of the Ministry of Defence (MOD) was embedded in an information and knowledge themed blog post in January 2017.

> A timely opportunity to assess the fitness of the knowledge and information management processes that support our decision making comes in the form of the upcoming Information Management Assessment (IMA) being undertaken by The National Archives.
>
> The National Archives conducts a programme of assessments to review information, records, and knowledge management standards within Government departments. To demonstrate our commitment I have asked The National Archives to carry out an IMA reassessment of MOD during February 2017. This follows on from a spot IMA in 2009, and a full IMA carried out in 2011. Reports of these assessments are available on The National Archives' website.
>
> The report that The National Archives produces will help to ensure that our information, knowledge and records are appropriately captured, managed and preserved, and information risks and sensitivities are appropriately handled – in turn, helping us to address some of the key lessons of Chilcot.
>
> My intention is that as well as helping to meet our corporate obligations to manage, protect and exploit the information we hold, everyone in Defence values our information and knowledge.

IMA background

- The first full IMA of MOD was formally closed in 2014. The IMA reassessment of MOD involved a detailed review of supporting documentation followed by interviews with senior staff, specialists and practitioners in London, Portsmouth and High Wycombe between 30 January and 7 February 2017. Additional interviews with key staff were conducted by telephone.

- This report provides a summary of the good practice and risks we identified focussing on high priority findings.

Executive summary

- There are ten performance headings embedded in this IMA report. MOD achieves four 'Satisfactory' ratings. The good practice and key highlights section below notes a number of positive approaches and changes implemented since the department's previous IMA.

- These range from MOD's use of the Holding to Account process as a basis for identifying gaps in information management capability to the department's inclusive interpretation of a record, as set out in its Records Management Improvement Plan. We also recognise the continued energy and effort applied to training provision for MOD's information specialists.

- The IMA report identifies six 'Development area' ratings aligned to our core recommendations. In particular MOD should:

    1. Address the lack of priority currently attached to information and records management at a strategic level. Establishing the right information management culture must be a priority if new systems are to be exploited effectively.

    2. Provide greater clarify on the delivery of key information and records management requirements by the new IT environment. MOD needs to establish how the gaps that exist will be addressed. MOD needs to articulate a clear vision for what good information management practice looks like in the Office 365 environment as a whole.

    3. Identify the steps needed to ensure the department's digital information remains complete, available and usable over time and through change.

    4. Continue to mature the department's approach to defining information and records management related risks. The role that the centre and Top Level Budgets (TLBs) are undertaking in mitigating these risks from a technical, governance and cultural point of view should be clearly set out.

    5. Continue to engage with The National Archives as it works to address the current limited oversight and understanding of the digital and paper records it holds. This is needed to support accurate reporting and so that MOD can ensure adequate legal cover is in place.

    6. Establish an agreed plan for compliance with the Public Records Act that encompasses disposal of the department's paper and its digital records.

- IMA reports and departmental action plans are published on The National Archives' website at: http://www.nationalarchives.gov.uk/information-management/our-services/ima-reports-action-plans.htm

Good practice and key highlights

The following are among the areas of good practice identified at the time of the assessment. They include approaches that other government organisations may find helpful in mitigating information and records management related risks:

Highlights of the 2017 IMA
• The Records Management Improvement Plan adopts a holistic definition of a record that includes, but is not limited to, structured information held in the department's EDRM. It notes: Although the plan necessarily refers to the MODNET programme and the records management capabilities on that infrastructure, all records irrespective of host platform are included in the scope of this plan. This would therefore include for example Human Resources Management System (HRMS) or Defence Medical Information Capability Programme (DMICP) systems.
• The Design Authority provides an avenue for assessing new or renewed IT solutions and identifying whether they are a strategic fit. It offers a means of influencing new projects from the outset. Information and records management related questions have been factored into the gateway process. This process places an emphasis on encouraging simple and reusable architecture.
• The central KIM team has established a KIM Working Group as a forum to develop a cross-departmental approach to knowledge and information management, and to drive engagement with KIM staff in TLBs.
• We saw evidence of business ownership of risk relating to compliance with information and records management policy. One TLB had defined a risk relating to information mismanagement with potential outcomes including poor information assurance, poor information exploitation and an inability to achieve operational advantage.
• MOD has continued to promote the training package it developed for all staff and to deliver role-based training to information specialists. In one location visited, information specialists stated that the courses they attended had provided a prompt to review and overhaul inherited information management plans.
• MOD is using the Holding to Account process to increase its understanding of information management maturity across the department, raising the issue at Senior Information Risk Owner (SIRO) level for each TLB. MOD plans to use responses to questionnaires sent out in the course of this process to generate tailored improvement plans for TLBs.

Recommendations to address risk areas

Full details can be found in Annex A (see pp. 12-15).

Recommendation 1
MOD to define, articulate and communicate strategic goals for information and records management, establishing a clear strategic vision.

Recommendation 2
MOD to ensure sufficient coverage of information management related risk within its risk management framework.

Recommendation 3
MOD to define how legislative and business requirements for information and records management will be met in the MODNET Office 365 environment.

Recommendation 4
MOD to establish a framework through which the right information management culture can be driven and maintained. MOD should ensure good information management principles are embedded in new ways of working to get the most out of the MODNET Office 365 environment.

Recommendation 5
MOD needs to identify how it will ensure the digital continuity of its information and records through to the point of transfer or destruction.

Recommendation 6
MOD to work with The National Archives to establish a clear, achievable and agreed roadmap for ensuring compliance with the Public Records Act, supported by mutually agreed working plans.

Key findings of the assessment

1 The value of information

Key developments since the last IMA:
• The MOD Information Strategy has been superseded by the Defence Information Strategy.[1] A new Records Management Improvement Plan has been produced.

Performance rating	
Communicating and realising value	**Development area**
Managing information as an asset	**Satisfactory**

- The 2016 Defence Information Strategy recognises the importance of good practice in information security and the need to exploit MOD's repositories of information and data. The strategy is IT focussed and strategic outcomes are to be achieved through the delivery of a single information environment. Information and records management receives comparably little attention, either as a goal in its own right or as a contributory factor that enables the achievement of others. The document makes no reference to the role of information and records management culture.

- We also saw no indication that the Defence Information Strategy and Records Management Improvement Plan are formally aligned.

- MOD needs to do more to establish why information and records management matters to the department. It needs to establish a strategic focus for work to improve and maintain standards if MOD is to get the most out of its new IT network. It should put in place proportionate strategic goals and a strategic vision for information and records management. These should be integrated with existing goals for IT improvement work and for the protection and exploitation of information and records. **See recommendation 1 and 4**

- MOD's size and complexity means that it has faced a significant challenge in adopting a proportionate and consistent approach for information asset governance. In general we found a good level of awareness of the importance of identifying and safeguarding information assets containing personal data. However, processes for oversight of business critical information assets, which were introduced at the time of the last IMA, do not yet appear mature.

- While we were pleased to note that some areas had taken the opportunity offered by our visit to put up posters reminding staff who their Information Asset Owner

[1] https://www.gov.uk/government/publications/defence-information-strategy

(IAO) was, guidance for IAOs dates from 2011. Its branding has not been updated to reflect internal changes in governance structures and it has not been reviewed in line with updates and amendments to the Security Policy Framework. **See recommendation 2**

2 Digital information and supporting technology

Key developments since the last IMA:
• MOD completed roll out of its Electronic Records Management System, Meridio. MOD has begun migrating from the Defence Information Infrastructure (DII) network to MODNET. It is introducing a cloud based service using Windows 10 and Office 365. • A central ICT design authority has been established.

Performance rating	
Supporting information through technology	**Development area**
Digital continuity and IT change	**Development area**

- The Defence Information Strategy drove the move to Office 365. This has included the adoption of SharePoint Online as successor to Meridio. Information and records management requirements do not appear to have factored significantly in this decision. We also note that the use of third-party plug-ins for SharePoint Online and on premise – of which there will be a limited parallel adoption – is not seen as a good fit for the department in view of the direction set by the Defence Information Strategy. It is not yet clear how effectively the new platform will meet the department's needs in areas such as retention scheduling, export, audit functionality and email integration. MOD's hope is that gaps will be dealt with through future platform updates. We saw no evidence of a 'plan B' if this does not happen. MOD needs to address this and should clearly set out how legislative and business requirements for information and records management will be met. **See recommendation 3**

- Roll out of Office 365 is progressing while MOD KIM and IT staff work to configure SharePoint Online to best effect. Staff are being encouraged to define new file structures, but are being asked not to enable records management functionality. While the move to SharePoint Online was a key priority in all areas we visited, some staff we spoke to expressed frustration over a lack of clear expectations that were being set for TLBs. There was also a significant amount of concern among interviewees about the potential impact of the move from role folders and role-based permission structures. This change, together with the removal of Outlook mailbox limits and the provision of increased online storage capacity via OneDrive will have an impact on the information and records management related risks that MOD faces. This may mean that TLBs have to invest more effort in ensuring their

staff capture and keep key information in shared areas in accordance with policy. **See recommendation 2**

- We are concerned that MOD is missing the opportunity to establish what good practice in information and records management looks like from the outset as its new IT environment is rolled out. As a consequence, embedded good practice behaviours may be being eroded and bad practice may be bedding in. At the same time as ensuring a supportive IT environment, MOD needs to invest significant effort to ensure the right information and records management culture is established and maintained. **See recommendation 4**

- MOD is carrying out a business-led migration of non-ephemeral legacy content from shared drives, existing SharePoint 2007 sites and Meridio to MODNET HP Records Manager. This is in preference to migrating this content into the MODNET Office 365 environment. A range of factors may increase the complexity of this process while raising risks to the digital continuity of the department's legacy information and records. These include inconsistent historic approaches to records declaration and varied adherence to required filing structures; the bespoke nature of MOD's SharePoint 2007 platform; a lack of insight into vulnerabilities caused by age and format of information held; the existence of multiple instances of HP Records Manager and the decision not to continue investing in enterprise search capability. At the time of the IMA no migration plan had been produced. MOD needs to ensure sufficient priority is given to this work. **See recommendation 5**

- MOD needs to plan to ensure the availability, completeness and usability of its digital information until the point of transfer or destruction. This includes legacy information and information that will be created in the MODNET Office 365 environment. It also includes operational digital information and information from other sources that cannot be stored elsewhere – for example, in HP Records Manager. MOD has identified a gap in capability in this area which the Records Management Improvement Plan aims to address. It should seek support from The National Archives as it works to identify a preferred solution. Related risks should be defined. **See recommendations 2 and 5**

3 Information risk, governance and oversight

Key developments since the last IMA:
• Information and records management related risk is no longer communicated at board level through the Information Risk Assurance Matrix. • The KIM Leaders' Working Group has been set up. • MOD's programme of internal information management assessments has ended.

Performance rating	
Recognising information risk	**Development area**
Establishing control	**Satisfactory**
Providing guidance	**Satisfactory**
Measuring impact	**Satisfactory**

- An information assurance strategy is in place. An information exploitation risk owned by the Chief Digital and Information Officer and SIRO highlights the reputational impact of an inability to access and exploit information at the right pace, quality and depth. However, this appears to focus on the DII rather than the MODNET environment. The only explicit reference to information management in the wording of the risk is in relation to a planned refresh of corporate policy. MOD needs to ensure that the potential risks raised by the new IT environment and information and records management practice are clearly defined. **See recommendation 2**

- While MOD has recently reviewed its appetite for information risk, its information risk policy dates from 2009. This should be revisited and updated. **See recommendation 2**

- The central KIM team has a policy focus and has traditionally been relatively isolated from the work of KIM teams within TLBs. Current and planned efforts to enable outreach activities, including through the KIM Working Group, deserve recognition and support. MOD needs to ensure that the same emphasis is being applied at a more senior level at the centre and within TLBs. This is needed to help drive work to embed the right information management culture. **See recommendation 4**

- The Defence Information Strategy underlines the challenge the department faces from a skills perspective in recruiting, retaining and developing the right people. An ICT focussed suitably qualified and experienced people (SQEP) strategy has been presented to the department's senior Information Board. There is an ambition to further extend this approach to the areas of information assurance and KIM. We support MOD's intention to review local information governance structures. Current structures are potentially effective, and were working well in a number of the areas we visited, but are not implemented on a consistent basis and are therefore unlikely to be delivering consistent value. MOD needs to address this and define what governance structures it needs once MODNET Office 365 is in place. **See recommendation 4**

- The central KIM team lacks oversight of documentation produced by TLBs covering the allocation of information management resources and definition of information management priorities. Information directives are still being produced, although there is no longer any formal requirement to do so after the closure of

the previous MOD Information Strategy. The contents and focus of locally created information management plans we reviewed varied. MOD needs to exert greater control in this area to ensure these are consistent and focussed in the right way. **See recommendation 4**

- Joint Service Publications for information and records management are significantly longer than most other departments' information and records management policies. MOD remains committed to making these documents more efficient and easy to understand. To help support and enable the right information and records management culture, MOD needs to establish what good practice looks like in the MODNET Office 365 environment and communicate this in a clear, consistent and straightforward manner. **See recommendation 4**

- The addition of a questionnaire covering both information management and management information (MI) to the Holding to Account process for the Defence Authority for Information offers MOD a new opportunity to drive good practice in TLBs. MOD should seek to tailor future questionnaires to known risk areas and to combine qualitative and quantitative insight. **See recommendation 4**

4 Records, review and transfer

Key developments since the last IMA:
• MOD has identified a significant backlog of paper records. MOD has over 9 million Service Personnel Records currently in legacy – for which there are nearly 450,000 records (pre-1902) not covered by a Retention Instrument (figure subject to change).

Performance rating	
Oversight of records and selection	**Development area**
Implementing disposal decisions	**Development area**

- MOD plans to take ownership of records in its main store back from TLBs to gain greater control. This is a key goal in the MOD Records Management Improvement Plan. While this is a positive, the volumes involved and varied control exercised over these records to this point raises a number of risks for MOD. In addition, there is a risk that significant volumes of legacy paper records may also reside outside the central archives in the UK and overseas. Although the central KIM team has sought to engage TLBs on this issue, a clear view on the scale of the problem has not been achieved. MOD needs to do more as a department to address this. It needs to be in a position to maintain and protect its paper records and must be able to account for and report accurately on its holdings. It needs to ensure that required legal cover is in place and should build on its own internal transfer plan, working with The National Archives to establish and deliver an

agreed roadmap for compliance with the Public Records Act. **See recommendation 6**

- MOD conducted an operational excellence exercise in 2015 looking at ways of improving processes for the appraisal, selection and transfer of historic records. It should engage with The National Archives to assess what further improvements could be made in the integration of best practice macro-appraisal methodologies. There is significant subject level expertise in the review team and we noted positive examples of knowledge sharing in relation to the sensitivity review process. MOD should build on this.

- MOD was a member of The National Archives' Digital Transfer User Group. It intends to begin transferring these to The National Archives in 2024 on the basis that its first Electronic Documents Records Management system was introduced in 2004. However, print-to-paper records management policies in place prior to this date may not have been fully adhered to. MOD may hold older digital information with historic value that should be selected for transfer to The National Archives. It needs to improve its understanding of its pre-2004 digital information. Care needs to be exercised in relation to the disposal of any information not moved across to HP Records Manager to ensure that records with business or historic value are identified. **See recommendation 6**

- MOD needs to continue to work with The National Archives to define requirements for digital transfer to ensure deadlines established under the Public Records Act are met. **See recommendation 6**

Annex A - Recommendations in full

Recommendations consist of an overall outcome to be delivered through the period of MOD's IMA action plan and a set of supporting actions that will help MOD address the recommendation.

Recommendation 1
MOD to define, articulate and communicate strategic goals for information and records management, establishing a clear strategic vision.
This would be supported by: • Embedding information and records management goals in the Defence Information Strategy or establishing a linked supporting strategy. Goals for information and records management and for the protection and exploitation of information should be linked. • Formally linking the Records Management Improvement Plan with the information management strategy.

Recommendation 2
MOD to ensure sufficient coverage of information management related risk within its risk management framework.
This would be supported by: • Ensuring that descriptions of information and records management related risks capture IT-related and cultural causes, and define mitigating actions for both (see **recommendations 3 and 4**). The increased burden that TLBs may need to bear in ensuring the right information is not held in personal spaces and is instead captured in shared spaces should be defined. • Defining the digital continuity related risk MOD faces. • Ensuring information and records management risks are within scope of current work to bring increased focus on information assurance risk. • Reviewing and updating information risk policy and information assurance strategy and ensuring these documents cover information and records management related risk.

- Reviewing and updating guidance for IAOs and setting clear expectations for the identification of information assets that do not contain personal information and data.

Recommendation 3
MOD to define how legislative and business requirements for information and records management will be met in the MODNET Office 365 environment.
This would be supported by: • Establishing a plan 'B' in case required functionality within SharePoint Online is not delivered through future platform updates. • Reassessing the benefit that might be obtained from the use of third-party plug-ins in areas such as email integration. • Reassessing the benefit that might be obtained from the proportionate application of technical controls to help address the risk that information stored in personal spaces will not be moved into corporate spaces. This is most likely to deliver benefit when coupled with efforts to improve ways of working. **See recommendation 4**

Recommendation 4
MOD to establish a framework through which the right information management culture can be driven and maintained. MOD should ensure good information management principles are embedded in new ways of working to get the most out of the MODNET Office 365 environment.
This would be supported by: • Ensuring that core policy principles for good information management practice in the new IT environment are clearly and simply defined and actively promoted to the business as MODNET Office 365 is introduced. There is a particular need to do so for key potential risk areas such as the use of OneDrive and the capture of email. • Drawing on good practice approaches from IMA members to target and improve specific ways of working (see Welsh Government and HM Treasury's work on email management).

- Establishing a clear vision for support roles and championing roles, with consideration given to professionalising roles. MOD should establish how key roles will help control and direct the creation and storage of information not only in SharePoint Online, but also in the wider MODNET Office 365 environment.

- Re-energising and formalising the framework through which TLBs allocate resources and plan. Required documents should be established on a consistent basis, aligned to departmental information strategy, and be subject to central quality assurance.

- Tailoring future assessments of TLB capability through the Holding to Account process towards identified risk factors. MOD should make use of qualitative and quantitative insight.

- Ensuring information and records management is referenced consistently in terms of reference documentation and feature on agendas of senior information governance boards at the centre, such as the three-star information stakeholder board and within TLBs.

Recommendation 5
MOD needs to identify how it will ensure the digital continuity of its information and records through to the point of transfer or destruction.
This would be supported by: • Ensuring legacy and current information is within scope. MOD needs a clear plan for the management of information moved into HP Records Manager through to appraisal, selection and transfer. Key considerations should include search, deduplication and identification of risks related to age and format. • Ensuring sufficient priority is given to the migration to HP Records Manager and that an accurate assessment of time and resource required from TLBs is defined. • Working with The National Archives to define how it will ensure the medium to long-term completeness, availability and usability of information from operations and from sources that cannot be stored in HP Records Manager.

Recommendation 6
MOD to work with The National Archives to establish a clear, achievable and agreed roadmap for ensuring compliance with the Public Records Act, supported by mutually agreed working plans.
This would be supported by: • Ensuring records held outside the main archive in the UK and overseas are identified. This needs senior support to ensure business engagement. • Reviewing the Records Management Improvement Plan to factor in IMA findings. • Continuing to work closely with The National Archives to reach compliance for the Service Personnel Records. • Working with The National Archives to establish a plan for the routine transfer of digital records. This should include identification of material that would benefit from transfer before deadlines established by the Public Records Act. • Identifying what material from earlier than 2004 is held and working with The National Archives to establish a plan for the disposal of information not moved to HP Records Manager. • Working with The National Archives to identify opportunities for the more effective integration of macro-appraisal principles. • Enabling more consistent knowledge transfer and knowledge sharing among the review team.