

# Information Management Assessment

---

Action plan progress  
review

Ministry of Defence

**Reviewed**

June 2014

**Published**

March 2015

Working with government  
to raise standards in  
information management

## **Overview**

The Information Management Assessment (IMA) programme is the best-practice model for government bodies wishing to demonstrate commitment to the principles of good information management.

The Ministry of Defence (MOD) IMA was held between 12 and 23 September 2011, with interviews at Whitehall offices, Permanent Joint Headquarters (PJHQ), Navy Command HQ, HMS Diamond, Navy Historical Branch and the Portsmouth Flotilla. The IMA report was published in June 2012. A detailed action plan was produced by MOD and progress against this was formally assessed in June 2014.

This review summarises key progress since the 2011 IMA and highlights areas where focus is still needed. Key developments include: a transformation in the way information risk is defined and documented, the inclusion of information and records management within the Holding to Account process, and the creation of the Single Information Maturity Model (SIMM) which promises a flexible tool for self-assessment and identification of future goals.<sup>1</sup> However, continued intense focus on information and records management will be required in the context of the realignment of information technology (IT) and information management functions. This is crucial for new systems to be trusted and well-used, and for MOD to realise the benefits of effective information and records management.

## **Key findings of the IMA 2011**

The original IMA report rated MOD as 'Good' under five out of 20 headings on the IMA performance framework risk matrix and 'Satisfactory' under a further 11 headings.

It specifically highlighted a number of areas of good practice. These included the MOD information strategy (MODIS), which received high-level endorsement and was scheduled for regular review. MOD had also introduced the 'Defence Information Management Passport', an e-learning package. This was intended to educate staff and raise standards in records and information management. Two locations visited

---

<sup>1</sup> The Holding to Account (H2A) process was developed with Commands/Top Level Budget (TLB) holders and process owners to support accountability on delivery of objectives within delegated budgets.

on the IMA made completion of the 'Defence Information Management Passport' mandatory before assumption of duties.

In addition, the original IMA report also identified four 'Development Needed' areas and made 17 recommendations for improvement. In response to this MOD produced a departmental IMA action Plan.

### **Context and progress against recommendations**

There are positive indications of MOD's continued recognition of the importance of good information and records management. At the beginning of 2013–14, MOD established information as one of six overall priorities. Its March 2014 departmental improvement plan also specifically highlights the need to improve standards of information management, stating: 'We recognise for information to be an asset and not a risk to Defence, we need to handle, manage and use it in the right way.' MOD should be commended for this clear statement of intent and for its openness in engaging on this issue. New leadership is also flagged: 'Challenging is an understatement, but we now have real clarity on the strategic issues we face and a new CIO to drive the work forward' (foreword, Departmental Improvement Plan).

The 2014 MOD departmental improvement plan highlights the core role that the Chief Information Officer (CIO) will continue to play internally in driving forward information priorities. In this context, this review notes that the central CIO organisation was subsumed within Information Systems and Services (ISS) in January 2014 and the role of CIO was filled on a permanent basis in spring 2014. A new joint IT and information management strategy is expected to be produced in 2015.

This progress review places a particular emphasis on the following key developments since the 2011 IMA:

#### **Information risk**

MOD has worked proactively to define and formalise its understanding of information and records management related risk in a way that can easily be reported at a senior

level, as a component of wider work to rationalise the department's risk management framework. The model adopted supports clear communication and continuity of understanding, and the detailed Information Risk Assurance Matrix that MOD has developed is an excellent model of how to capture risk and define actions arising.

The matrix breaks down information and records management related risk under headings such as leadership, policy and guidance, culture and skills and IT tools. It is updated annually and presented to the Defence Board. Mitigating activity is plotted against each risk – for example, the need for training, updating policies or behavioural change – thus recognising the multi-faceted nature of both the risk and the ways of addressing it.

### **Records Management and strategic impetus**

MOD is currently placing an understandable strategic emphasis on improving technology provision. This is important from an information and records management perspective as well as a business one. However, while a supportive technology environment is crucial in removing key barriers to records creation, IT should not be regarded as an end in itself. MOD must ensure a continued focus on the information and records that technology should be supporting. This is important because, with new governance arrangements in place, MOD has the opportunity to produce a truly integrated strategy and vision for information and records management and IT.

### **MOD's programme of internal IMAs and the Single Information Maturity Model**

Management controls were identified in the original 2011 report as a 'Development Needed' area, in part because no assessments within the department's own internal programme of IMAs had been conducted that year.

MOD has since carried out two internal IMAs: the Strategic Weapons Project Team (SWPT) in the Defence Equipment and Support (DE&S) top level budget (TLB), and the Atomic Weapons Establishment. However, no further internal IMAs have taken place and none are currently planned.

This review recognises the Single Information Maturity Model (SIMM) as a useful and promising tool for assessing performance and driving improvement that should

have wider impact across the organisation than a number of small internal IMAs if taken up and used as currently proposed. MOD should be commended on the development of the model and encouraged to pursue its piloting and implementation across the organisation. Designed to be a flexible self-assessment tool that will feed into the department's Holding to Account process, it is, however, as yet still unproven.

The application of the SIMM is particularly important because reporting tools have yet to be rolled out to provide local and central oversight of performance in information storage and records creation. This was a key area of concern raised in the original IMA report. Without these, MOD cannot easily make a granular assessment of how new systems – and any alternatives – are being used, or establish a baseline.

### **The Holding to Account process**

The original IMA report highlighted concerns over the consistency with which MODIS was interpreted within individual TLBs. TLBs now no longer write their own information strategies, but are expected to produce information directives and comply with information and records management requirements: this is assessed as a component of the wider Holding to Account process. The first report that we had sight of (May 2014) gives a frank overview that captures key issues for each TLB, and MOD is to be commended for the openness with which issues are set out. This review notes, however, that action points, although clear and well signposted, are quite broadly defined and allocated to Information Systems and Services rather than to TLBs. In addition, although an escalation route has been defined, it was not used in this instance.

This is a particular concern where significant gaps are identified in relation to TLBs, such as decisions not to produce information directives or end-of-year reports, or to commission IT equipment independently. In the former case, no specific action point is defined. In the latter case, the stated response relates only to improved future provision of IT by ISS.

## **Information Management Passport**

Changes have been made to the way the Information Management Passport is delivered, condensing the time allotted to training. The proposed separate passport for senior staff has not been developed, but the aspiration is to offer master classes instead, and the passport itself now consists of two hours of training rather than four.

## **Electronic Document and Records Management System (EDRMS) roll out**

Records creation and storage were identified as 'Development Needed' areas in the original 2011 IMA report. The roll out of MOSS (Microsoft Office SharePoint Server) and Meridio (MOD's EDRMS) is ongoing ('Secret' level to be rolled out in August 2014).

- All of MOD except Defence Infrastructure Organisation (DIO) has enabled the use of MOSS. DIO was identified more generally in the Holding to Account report as at risk in relation to identification and management of information assets, so central oversight is required here to support the roll out.
- The search function had been disabled in MOSS because of security concerns, and as a consequence there may be some impact on users' trust in the system that needs addressing as the roll out continues, especially with highly sensitive information.
- New systems are expected to reduce the burden on users, but will not remove it entirely, and concerns remain in key areas such as email capture.

## **Selection of historical records**

MOD reported that it had identified a total of 48,925 legacy records in the spring 2014 Records Transfer Report (RTR), one of the highest numbers reported among government bodies that transfer records to The National Archives. MOD's response to the RTR indicates that this number may increase if further records sets are identified. MOD has a programme of work in place in relation to out-of-time records, but continued focus and emphasis is needed on this issue. This review notes, for example, that there has been no significant progress in assessing the status of records held by Naval Historical Branch, which was one of the recommendations in the 2011 IMA report.

## **Knowledge management**

Knowledge management was identified as a 'Development Needed' area in the 2011 IMA. An independent review of knowledge management initiatives within MOD and its agencies was carried out in 2013. This identified what knowledge management can achieve ('increasing knowledge re-use, identifying knowledge gaps and increasing the quality and speed of decision making') together with commonly occurring barriers (for example, lack of uptake, lack of reinforcement, cultural practices that inhibit knowledge sharing). A number of initiatives are underway – such as knowledge cafés – which are intended to focus on available tools and benefits, and the KIM Workforce Development Plan will be key to delivering these. This review also notes that there is now a knowledge stream within the Defence Learning Strategy. This remains a work in progress but MOD's progress to date is recognised.

## **Next steps**

The National Archives will continue to work closely with MOD so that the department is supported as it continues its work on records and information management. It is recommended that MOD focusses on the following:











- It is crucial that the priority so far attached to the Records Management Improvement Plan is maintained. Key lessons learned should be incorporated into strategy going forward.
- MOD should ensure that its focus on information risk is maintained so that the audit committee can track and interrogate the impact of strategy in reducing threat and enhancing opportunity.
- In combination with the use of the SIMM, MOD must now provide a clear plan on the use of reporting tools: identifying, for example, what will be monitored, how this information will be reported and used and what action will be taken as a result. Without metrics on records creation, it will not be clear to MOD whether systems are being used optimally and records are being created routinely in line with policy.
- Reporting on compliance with information and records management requirements within the Holding to Account process has had clear benefit,

particularly in positioning performance in this area as a core business issue. MOD must ensure, though, that sufficient emphasis is given to compliance and that there is robust follow-through. MOD's approach to documenting information risk demonstrates its understanding of the significant impact that a lack of information availability can have. As a component of mitigating that risk, it must drive consistent interpretation and application of information and records management principles across TLBs.










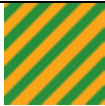














- MOD must continue to invest effort in culture change across TLBs as new IT systems are adopted. This is crucial to ensure that information is created, stored and shared correctly, both for daily work and for the future record.
- MOD needs to understand the number and age of records held to support compliance with the Public Records Act and to ensure that records are stored, disposed of or subject to a Lord Chancellor's Instrument (LCI) as required.







Progress against on-going areas of concern raised in this review will be revisited at the time of the next formal IMA in 2016/17 and monitored via standard meetings with the departmental Information Management Consultant (IMC).






#### IMA risk matrix

<b>Governance and leadership</b>	<b>Assessed 2011</b>	<b>Reviewed 2014</b>
Strategic management		
Business objectives		
Management controls		
Resourcing		
Risk management		



<b>Records management</b>		
Creation		
Storage		
Appraisal, disposal and transfer		
Management		
Digital continuity		
<b>Access to information</b>		
FOI/Data protection		
Re-use		
Security		
<b>Compliance</b>		
Staff responsibilities and delegations		
Policies and guidance		
Training		
Change management		
<b>Culture</b>		

Commitment		
Staff understanding		
Knowledge management		

Key to colour coding	
	<b>Best Practice</b>
	<b>Good</b>
	<b>Satisfactory</b>
	<b>Development needed</b>
	<b>Priority attention area</b>