The National Archives

# Information Management Assessment

## The Ministry of Justice

### June 2011

Date: June 2011

# PART ONE: EXECUTIVE SUMMARY

1.1 The Ministry of Justice (MoJ) is a large, complex and relatively new department created through a series of mergers, and thus faces unique issues in building integrated information management systems, processes and culture. It creates a wealth of information, which is largely stored on legacy and bespoke systems. Data quality and integrity of information have a major impact on policy-making and reporting. This can lead to inefficiencies and risks. As the department moves into a tough cost environment, the challenge for MoJ is to manage the risks around information management.

**Governance and Leadership**

1.2 MoJ has prepared the ground for effective corporate structures to manage its information. It has established robust policy and guidance frameworks and is taking steps to tackle the many information management challenges facing the department. Examples include establishing closer working arrangements between Knowledge and Information Management (KIM) and Information and Communications Technology (ICT). However, many of the business areas assessed did not adhere to the policy requirements, leading to local practices and a lack of consistency. Although there was clear evidence of good local KIM practice, this was not consistent and good practice was not shared across the organisation.

1.3 Recommended priority action areas:

- KIM team and ICT to establish better links and work more closely in establishing policies and developing systems. This will better support effective information management.
- Reduce the habit of directorates practising localised information management by establishing consistency across divisions and clear instructions to default to corporate systems where available.
- Active and continual support at board level, cascaded to directorate level, especially within the context of the 2011 Comprehensive Spending Review

and Transforming Justice programmes. This should be supported by a network of KIM professionals, to ensure that KIM policy is properly applied.

- Address the confusion of post-holders and staff about the role and remit of the different information management roles within MoJ.
- Broaden the definition of information risk to encompass more than just the security risk, such as the risk of not sharing information effectively.

**Records Management**

1.4 MoJ creates vast amounts of information, which is stored in numerous legacy and bespoke systems across different platforms and formats. Many of these systems work well and are effective in isolation in their own business areas.

1.5 Recommended priority action areas:

- Ensure that staff wishing to work collaboratively, for example on Sharepoint, Huddle or Civil Pages, are not duplicating their efforts on separate systems, as this is uneconomic and may put continuity of digital information at risk.
- Manage negative staff perceptions of the systems for the storage of information. Both MoJ HQ and the National Offender Management Service (NOMS) have an extensive range of different, incompatible systems and locations for the storage of information. These are often perceived to be unstable, unreliable and difficult to use by staff. This creates a challenge in managing data quality and integrity, which can impact on policy-making and reporting.
- Library services to continue a move towards greater use of electronic journals and publications, subject to availability and licence restrictions.
- Implement ‘What to Keep’ policies and training for staff. Many of the staff interviewed were keeping far more information than necessary. This is not a tenable or effective policy, leading to additional storage costs and difficulty in searching and retrieving information.
- Ensure that operational data is collected, updated and stored to enable reliable statistics, and that best practice information management

approaches – for example, in the context of Lean programmes – are shared.[1]

**Information Access and Re-Use**

1.6 MoJ has effective data protection, freedom of information and information assurance processes and policies in place.

1.7 Recommended priority action areas:

- Ensure consistency in staff training on data protection. Staff at MoJ HQ demonstrated a thorough understanding of the Data Protection Act (DPA). However, good practice was not uniform, with storage of information about individuals, such as staff sickness and absence records, on personal drives.
- Raise awareness of the risks under the Freedom of Information Act (FOIA) and DPA if the existence and whereabouts of information is unknown. Information held in legacy systems with free text fields could present additional difficulties.
- Focus on strengthening the structure of the NOMS intranet.

**Compliance**

1.8 MoJ has recently revised much of its information management guidance, although this is not always easily accessible. There are a number of specialist KIM roles in place across the organisation that could be used to manage information more effectively. While figures indicate that all staff have completed the mandatory Cabinet Office e-learning package on Information Assurance, it is evident that understanding of data security issues could be better in some areas.

1.9 Recommended priority action areas:

- Utilise Information Managers (IMs) to assist the business areas in managing their information.

[1] The application of Lean principles in MoJ aims to achieve real and sustainable change by empowering staff to use their knowledge and creativity to remove waste and simplify systems.

- Improve records management guidance within MoJ so staff know where to turn for help. Ensure that guidance it is easily accessible via the intranet.
- Protective marking was not universally understood across MoJ. Local attempts to make guidance more comprehensive appeared successful in areas such as the Shared Service Centre, but a more standardised approach is needed together with approaches such as the 'Compliance Passport' approach to training.
- Ensure that adequate controls are in place to define contractors' KIM responsibilities.
- Ensure that all staff complete the refreshed e-learning package on Information Assurance.

**Culture**

1.10 MoJ HQ and NOMS continue to have strong individual cultures. There is a commitment to enabling better sharing of information across the organisation, and to building a greater understanding of the importance of KIM among staff and of the benefits it can bring.

1.11 Recommended priority action areas:

- Integrate information management practices within the department's larger agencies. The lack of a fully utilised corporate information system and the inability to technically share information across MoJ represents an obstacle to free sharing of information. Staff and teams frequently regard corporate information as their own.
- Increase understanding across the department of the value of information as an asset and the risks of failing to manage those assets properly.
- Establish consistency over the capture of knowledge of staff and contractors before departure. Good practice in some areas could be rolled out across the department.

**Risk Matrix**

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

**Governance and Leadership**

| | | |
|---|---|---|
| Strategic management |  | |
| Business objectives |  | |
| Management controls |  | |
| Resourcing |  | |
| Risk management |  | |

**Records Management**

| | | |
|---|---|---|
| Creation |  | |
| Storage |  | |
| Appraisal, disposal and transfer |  | |
| Sustainability of digital records |  | |
| Management |  | |

**Access to Information**

| | | |
|---|---|---|
| FOI/Data Protection |  | |
| Re-Use |  | |
| Security |  | |

**Compliance**

| | | |
|---|---|---|
| Staff responsibilities and delegations |  | |
| Policies and guidance |  | |
| Training |  | |
| Change management |  | |

**Culture**

| | | |
|---|---|---|
| Commitment |  | |
| Staff understanding |  | |
| Knowledge Management |  | |

| Key to Colour Coding | |
|---|---|
|  | **Best Practice** |
|  | **Good** |
|  | **Satisfactory** |
|  | **Development Needed** |
|  | **Priority Attention Area** |

PART TWO: INTRODUCTION

## Information Management Assessments

2.1 The Information Management Assessment (IMA) programme is the best practice model for government departments wishing to demonstrate a high level of commitment to managing their information. The IMA programme is a key element of that function.

nationalarchives.gov.uk/information-management/our-services/ima.htm

### Background

2.2 The Ministry of Justice has grown dramatically in the last twenty years, evolving from the Lord Chancellor's Department – a small department with responsibility primarily for the courts – to a large department of state with wide-ranging responsibilities and significant public visibility. This has happened partly as a result of the creation of new policy responsibilities, such as Freedom of Information (FOI), but more commonly by the transfer of functions from other departments. This growth has had some consequences for the department's information management.

2.3 The National Offender Management Service (NOMS) was created in 2004 by a merger of the headquarters of the Prison Service and the Probation Service, with the intention of creating a body that would be responsible for oversight of the management of an offender for the entirety of his or her sentence. In 2007, responsibility for the service was transferred from the Home Office to MoJ. In 2008 it became an executive agency of MoJ and took over direct responsibility for all operations of the Prison Service and the Probation Service. As an executive agency it is responsible for managing its own finances and developing its own policies and objectives, under MoJ guidance.

### Knowledge and Information Management at the Ministry of Justice and National Offender Management Service

2.4 The Knowledge and Information Strategy Division at MoJ consists of two arms. The Records Management Service (RMS) provides records management services to MoJ HQ, Her Majesty's Courts Service (HMCS),

the Tribunals Service, the Coroners' Court and various associated offices. The RMS team is responsible for registry services, outsourced archival services, the review team and policy and education. The Knowledge and Information Management (KIM) team has responsibility for developing MoJ KIM strategy and vision and also comprises the EDRM records management and EDRM business customer support teams.

2.5 Information management policy within NOMS is the responsibility of the Information Management team within the performance information and analysis group. The Information Management team is also responsible for records management, information retention and data quality policy. At the time of assessment the team consisted of two permanent members of staff and two contractors, together with a team of file reviewers. Day-to-day business includes the operation of the Local Information Manager (LIM) network and responding to information management queries. Ongoing projects include HQ Electronic Records Management project (HERM), culture transformation and file and paper management.

# PART THREE: ACTIVITIES CARRIED OUT BY THE ASSESSMENT TEAM

3.1 The assessment took place took place between 28 June and 9 July 2010.

3.2 Each IMA is conducted by members of the Standards team at The National Archives, accompanied by expert colleagues selected to meet the requirements identified in the pre-assessment planning. For this assessment, the team comprised:

- Standards and Assessment Manager
- Head of Standards
- Head of Information Management and Practice
- Standards Adviser
- Information Management Consultants
- Digital continuity project members
- Information Policy Consultants

**Scope of IMA**

3.3 The Ministry has engaged with the Information Commissioner recently on its Freedom of Information and Data Protection compliance, the latter in the course of a formal audit. The IMA did not therefore consider these areas in any depth.

**Assistance provided by the Ministry of Justice and the National Offender Management Service**

3.4 The assessment team are grateful for the co-operation and assistance of all MoJ and NOMS staff who were interviewed, provided additional information or facilitated the assessment process.

# PART FOUR: HIGHLIGHTS AND AREAS FOR IMPROVEMENT

## Governance and Leadership

### Strategic Management

4.1 The value of Knowledge and Information Management (KIM) is not universally appreciated across MoJ. Several of the KIM staff interviewed did not believe it to be regarded as business critical by senior management. It is important that the team addresses this as part of the KIM strategy, ensuring that there is active and continual support at board and directorate level, which translates into action throughout MoJ to ensure that KIM aims and policies are met.

**Recommendation 1: MoJ to demonstrate active and continual support of KIM at board level which is effectively distilled throughout the organisation.**

### Business Objectives

4.2 The assessment team found many examples of excellent practice in the handling of information, but all too often that practice was confined to a particular directorate or division and was the result of local initiative. If MoJ is to benefit from such initiatives, there must be mechanisms by which good practice can be applied across the board. It is vital for good information management that there is one record of policy decisions and that data and information is shared effectively across boundaries. Reinforcing the policy leads and responsibilities across MoJ will demonstrate robust KIM leadership.

**Recommendation 2: The KIM team to collate and share examples of good KIM practice across the department.**

### Management Controls

4.3 Currently, directors and heads of division may opt into using the corporate systems, such as the electronic document system TRIM. There is therefore no consistency of use across MoJ. The decision of whether to

use corporate information management systems or not can change with each change of manager. There is a clear and urgent need for explicit direction from the senior management of both MoJ HQ and NOMS that a set of agreed procedures and processes are put in place to manage the organisation's information. Without this there is the risk that key information is lost or inaccessible.

**Recommendation 3: MoJ to provide clear guidance on the use of corporate information management systems, ensuring that their use is part of internal governance processes.**

**Resourcing**

4.4 The KIM team at MoJ HQ has undergone a series of changes to enable it to meet the information management challenges of a growing department. The KIM team needs to have the visible support of the board and senior managers from across the department, in order to set up an effective governance structure to ensure that processes and recommendations are followed. The KIM team has to be positioned so that it is seen as the 'go-to' team within MoJ, as the lead on knowledge and information management and records management issues. Staff members interviewed were often not aware of whom to contact if they had a particular information or record management query. Without this clarity, there is the risk that inefficient KIM practices will continue and pose a significant long-term risk to MoJ and NOMS, for instance that information is lost, not saved or inaccessible.

**Recommendation 4: The KIM team to publicise its role to ensure that staff know who they should approach for help on KIM.**

4.5 Historically, different teams in MoJ have been responsible for the systems used for storing information and the management and policy lead on the information itself. This lack of coordination has led to issues in how systems are used. The KIM and ICT teams must work together to ensure that any relevant new or revised systems incorporate considerations of how information within the systems is processed or produced to support effective long-term information management. The policy lead for all information management matters must be seen to lie with the KIM teams,

not with ICT. The assessment team have subsequently been advised that the KIM team are working closely with ICT on relevant projects for MoJ.

**Recommendation 5: MoJ to ensure that all relevant ICT projects include information management considerations, working in conjunction with the KIM team.**

4.6 MoJ HQ and NOMS have several roles that support KIM and information management. These are Information managers (IMs), Local Information Managers (LIMs) and Knowledge and Information Liaison Officers (KILOs). Many of those interviewed were new in post.

4.7 The IM network has historically been responsible for supporting maintenance of the TRIM EDRM system; expanding their remit to encompass wider information management would add much needed support to the work of the KIM team. All staff across MoJ have responsibilities to manage their information well. This should be with the support of the network of skilled information managers.

**Recommendation 6: MoJ to reassess the IM role to ensure they support the KIM agenda more effectively and their responsibilities are cascaded throughout the department.**

**Risk Management**

4.8 MoJ is, via the information asset register, working to identify its information assets. In some instances, however, there is still some inconsistency in the definition of an information asset. In places, an asset has been identified as anything that contains information and is not limited to specific bodies of sensitive, business critical or personal information.[2]

4.9 Once identified, the KIM team should work with Information Asset Owners to ensure that the value of all information assets is ascertained. To achieve this, the KIM team needs the authority to ensure that standards are understood and applied across the board.

[2]Guidance on defining information assets can be found in section 3.1 of *Identifying Information Assets and Business Requirements*. http://www.nationalarchives.gov.uk/documents/information-management/identify-information-assets.pdf.

**Recommendation 7: MoJ to continue to identify and define its information assets, raising awareness of their importance and responsibilities among key staff.**

4.10 MoJ has an established system of Information Asset Owners, but they are not fully effective in the two organisations assessed. Information Asset Owners need to understand the full use of the information assets so that they can ensure the integrity of information assets throughout their lifecycle. The identification of an asset requires recognition of risks associated with it. NOMS is particularly well-attuned to the risks associated with information security: the loss or unauthorised release of data relating to offenders could have serious consequences for the organisation and especially for individuals. These risks are understood by those responsible for KIM in MoJ HQ and NOMS, but the assessment team did not see evidence that they are given adequate recognition elsewhere.

4.11 MoJ HQ has a network of Senior Information Risk Owners (SIROs) with a clear understanding of the breadth of their role, and with responsibilities spanning information assurance and information management in addition to information security. This places them in a strong position to manage risks to the continuity of their digital information.

4.12 At the time of the onsite review, NOMS had an interim SIRO whose focus was the management of physical risk, and the risk of inappropriate disclosure of information. The department will remain exposed to digital continuity risks until information risks are owned at the correct level and given sufficient priority. NOMS has since mitigated this risk as the current SIRO is also director of ICT.

**Recommendation 8: NOMS to extend the definition of information risk to cover risks to the completeness, availability and usability of digital information.**

## Records Management

5.1 MoJ is a large, complex and diverse department that creates vast amounts of information. This information is located in numerous legacy and bespoke systems, across different platforms and formats. Both MoJ HQ and NOMS have difficulty fully exploiting their information because it is not readily accessible. Difficulty also arises when having to work across diverse systems or functions that are not interoperable, and where staff can opt out of using the corporate systems. The numerous systems have a further impact on data quality and integrity, which if left unmanaged can have an effect on policy-making and information reporting.

### What to Keep/Creation

5.2 MoJ creates an abundance of information but this could be better managed. Staff at MoJ HQ and NOMS have a tendency to keep far more information than is necessary, 'just in case'. This is not a tenable or effective policy. Only those files that should be preserved, for example as records of decisions, as records of the operations of the organisation or as records of the development of policies, should be kept in perpetuity. Elsewhere there was evidence that local decisions were being taken on what material is to be destroyed. This was particularly evident in the case of email management, where the lack of effective policy revealed a variety of techniques in the retention and disposal of emails, which could result in valuable information being lost.

5.3 A 'What to Keep' project, to determine MoJ's disposal and retention policies for all information held, is vital to the effective and efficient running of MoJ HQ and NOMS. The decisions on what information is to be kept will need to be communicated to staff so that they have a clear idea, when deciding whether to store information in corporate systems, of what is important to the organisation and what is ephemeral. Effective implementation of this will need the support of local information management specialists.

**Recommendation 9: MoJ to implement a 'What to Keep' project, with the support of The National Archives, to implement 'What To Keep' guidance.**

### Storage

5.4 Both MoJ HQ and NOMS have an extensive range of separate, often incompatible, systems and locations for the storage of information. These include paper files, email inboxes, personal computer drives, legacy systems, team shared drives and corporate systems.

### TRIM

5.5 The corporate electronic document system in MoJ is TRIM. It is currently unsupported by MoJ's service provider and, in order to work effectively, would need to be upgraded at least to the next version of the system, but ideally to the latest version available. It will take significant effort to mend the reputation of the system so that it is trusted and used consistently by staff across MoJ. There are currently some teams that do not use TRIM, which puts the corporate record at risk. However, an initial analysis of upgrading the system indicates that it would be prohibitively expensive to do this, and so the department needs to evaluate the appropriate way forward. MoJ may need to adopt an interim solution of more rigorously structured and monitored shared drives, in tandem with making the best use of the current version of its EDRM where it is in used by its staff.

**Recommendation 10: MoJ to evaluate its options for corporate information storage, assessing its EDRM capability and the potential for more rigorously structured and monitored shared drives to meet its needs.**

### HERM

5.6 The HQ Electronic Records Management project (HERM) is currently being rolled out at NOMS main offices. This is an Approved Shared Drive (ASD) rather than an Electronic Document Record Management System (EDRMS) and offers a functionally based file structure on the new H-Drive and access controls. LIMs have a key role to play as gatekeepers, ensuring that folder structures are adhered to and controlling creation and deletion of folders.

5.7 New folders are created on receipt of a completed request form approved

by the team's LIM and recorded on a central Excel spreadsheet. A limited amount of metadata at folder level can also be recorded, such as owner, scope and key for closure.

5.8 Teams in the process of moving to HERM are encouraged to use the H-Drive exclusively. The decision on whether to migrate existing caches of information and historic files is to be taken by individual business units. Staff who have used HERM seem confident in the new system.

**Management**

5.9 Both TRIM and HERM offer the ability to share information based on a corporate standard approach. Outside these systems, the use of local shared drives indicates that sharing information adds value to that information and subsequently benefits the organisation. However, among staff using a particular shared drive, there is inconsistency as to how they use the drive, where they store material and what they call it. The assessment team found evidence that members of staff in both MoJ and NOMS had on occasion encountered difficulty in finding information, including the basis of previous policy decisions. Individual rather than corporate approaches to storing information will impact on the ability of staff to share information and there is a real risk that MoJ's corporate memory will become dispersed, and that business-critical information will become inaccessible or be lost when staff leave or when business areas are restructured.

**Paper files**

5.10 Paper records are still used across MoJ. In some areas this is due to reliance on historic records, the need for signatures, the need to exchange information in hard copy with other bodies whilst in other areas there is a preference for paper records. This affects interoperability between systems.

5.11 Within prisons, hybrid paper and electronic records persist, despite the introduction of the Prison Service Offender Management System (Prison-NOMIS). A number of records relating to the management of offenders' sentences are generated in hard copy only, with the result that the offender record continues to be pieced together from multiple sources.

5.12 Within NOMS headquarters, the assessment team evidenced files open up to 11 years after they were created. At the time of the assessment there was pressure to reduce the volume of paper records ahead of the NOMS office move.

**Recommendation 11: MoJ and NOMS to assess and mitigate the ongoing risk of managing and handling prisoner records from a number of sources.**

**Emails**

5.13 Emails are now the principal medium of communication and can include information which is essential to the organisation: background on the creation of policy, records of decisions taken, advice and key documents are all transmitted by email. It is essential that those messages with ongoing business value are preserved and accessible for future use. A high proportion of interviewees across MoJ treated the contents of their personal inboxes as their own records and stored them as such. Others converted emails to PST files, which were then stored on their PCs. Such practices restrict or prevent access and can lead to loss of data when individuals leave. MoJ could be at risk of failing to meet obligations under both DPA and FOIA if it is not able to find information stored in the emails.

**Recommendation 12: Staff must be instructed to store corporate information in the appropriate system. Technical controls should be considered to minimise the risks.**

**Sustainability of Digital Records**

5.14 MoJ has a large number of ICT systems, which are not all interoperable and staff often have the choice of which system to use. There is currently a move towards shared solutions with greater onus on suppliers to understand and respond to business requirements. It is essential that KIM requirements are understood and embedded in any future changes to information systems.

**Recommendation 13: The ICT function should work in partnership with KIM and business units to support good working practices, and ensure**

**that technology meets requirements for the completeness and availability of information.**

**Recommendation 14: MoJ should continue its programme of rationalising and consolidating the technology supporting the business.**

**Recommendation 15: MoJ should continue to take active steps to phase out the use of duplicate systems and databases, decommissioning redundant technology.**

### Change management

5.15 The MoJ Acceptance into Service (AIS) checklist was revised in 2009 to incorporate Data Management and Records Management criteria. However, the assessment team found little evidence that information requirements were fully considered as an integral element of the change management process. Projects must consider KIM factors from the outset – both when defining requirements and in establishing success criteria for the project as a whole.

5.16 In NOMs individual business units are tasked with and encouraged to migrate their own information into HERM. Keeping legacy information systems operational presents digital continuity risks. At the same time, transfer of material needs to be managed carefully to ensure that the context of the digital information remains understandable by other users.

**Recommendation 16: MoJ should ensure that ICT-enabled change projects conduct a formal impact assessment on the completeness and availability of information.**

5.17 ICT solutions must support good information management, including:

- Minimising the exposure of the organisation to digital continuity risk through streamlining the ICT infrastructure and reducing the number of systems and technologies in use.
- Requirements for data interoperability or cross-organisational collaboration, considering open standards where appropriate.

- Managing the lifecycle of legacy and ageing ICT systems, planning when and how to decommission them.

**Recommendation 17: MoJ to continue providing access to digital information as a key requirement for projects, expressed in terms of meeting business requirements for using this information.**

**Recommendation 18: MoJ and NOMS to agree a process for managing risks to the continuity of digital records.**

### Appraisal, disposal and transfer

5.18 Where disposal occurs, defined criteria should be applied to digital and paper files to ensure that information that should be retained is not being destroyed. The assessment team found evidence that this did not always occur in a number of areas due to time pressure. In other areas, local or individual criteria were being applied.

5.19 At the time of assessment, staff within NOMS HQ were investing considerable effort in reducing the massive volume of accumulated paper records. The published objective was to ensure that volume was reduced and that records were transferred to the appropriate registry. The assessment was supported by comprehensive guidance, which included information on what information should and should not be kept, scanning and secure disposal. The guidance also reinforced the registered file system. This work will provide the foundation for underpinning a more comprehensive MoJ 'What To Keep' protocol.

**Recommendation 19: MoJ and NOMS HQ to extend guidance on what information is critical to the business until a sustainable 'What To Keep' protocol is in place.**

### Prison NOMIS

5.20 The aim of Prison-NOMIS, which went live across prisons in May 2010, is the provision of single custodial records for life. It contains case notes, as well as personal information, and differs from its predecessor in being a centralised database with real-time access to information. New

prisoners are allocated a unique NOMIS number, against which further records should be associated if an offender is subsequently reconvicted.

5.21 Prison-NOMIS is intended to help standardise procedures, increase efficiency and coordination and is likely to be of wider benefit beyond the prison service in, for example, providing read-only access to offender information to the Probation Service. However, a number of gaps remain. Prison-NOMIS does not extend to privately run prisons. When an offender moves to a private prison they are accompanied by a print-out of the information from Prison-NOMIS, which will be entered on to the local inmate database system by a member of Her Majesty's Prison Service staff.

5.22 The range of information entered onto Prison-NOMIS varies between prisons. Unless information is entered in a uniform way there is a risk that the value of the information will vary depending on where it was entered.

**Recommendation 20: NOMS to issue guidance for standards of data entry into Prison-NOMIS to enable consistency.**

**Data Quality and Integrity**

5.23 The effort within NOMS to ensure the collection and availability of high quality data about its operations and the existence and ease of use of the performance hub to coordinate this is commendable. However, within MoJ HQ there is a lack consistent approach to managing some information for example, performance information about the operation of the courts. This may result in management information and statistics being unreliable, which could have an impact on policy development and decision-making.

**Recommendation 21: MoJ to provide support and reinforce guidance on ensuring that operational and service information is complete and accurate.**

## Access and Re-Use of Information

### Data Protection Act (DPA)

6.1 Staff within MoJ HQ demonstrated a thorough understanding of the DPA. This is to be commended. However, the assessment team found areas where information about individuals, such as records of staff sickness absence, is kept on personal drives, which is not good practice. Increased liaison between KIM staff and those responsible for data protection could improve the situation. NOMS is currently working to address some DPA related issues it has itself identified.

**Recommendation 22: KIM team to reinforce guidance to staff on maintaining sensitive personal information.**

### Freedom of Information Act (FOIA)

6.2 The Data Access and Compliance Unit (DACU) within MoJ has recognised the need for better KIM across the department and has therefore introduced a programme of working with teams to improve practices. Further difficulties are presented by legacy electronic systems that contain information in free text fields, which are not easily searchable.

### Re-Use

6.3 MoJ information is currently made available for free re-use via The National Archives' PSI Click-Use Licence.[3] There are therefore no restrictions in place, which is good practice.

6.4 MoJ has published a total of 125 datasets on data.gov.uk, of which 23 new datasets were added since May 2010.[4] They are one of the leading government departments in terms of supplying datasets directly. MoJ is currently developing a transparency plan, to be published mid-September 2010, and has developed a three-step approach:

[3] The PSI Click-Use Licence has now been superseded by the Open Government Licence (OGL).

[4] Figures correct to August 2010.

- delivering the commitment to transparency (HR, contract, spending)
- identifying and publishing performance data (MoJ's Information Strategy)
- defining a release schedule of MoJ datasets led by public demand.

This is an example of best practice.

**Security**

6.5 NOMS has given a high priority to data security, although the predominant use of paper files in prisons is a risk. Data security in the prison system is also challenged by the requirement to share information extensively with other agencies, such as the police and colleagues in the Probation Service, often via fax. Prisoners' information can be held on a number of files and systems. Prison-NOMIS should help NOMS to manage its information effectively, safely and efficiently. The team responsible for tackling information assurance risks within NOMS is reduced in size. NOMS need to ensure that it retains the ability to be proactive in managing its emerging and ongoing information assurance risks.

**Recommendation 23: NOMS should give careful consideration to how it devolves responsibility for information assurance to local offices.**

## Compliance

### Staff responsibilities and delegations

7.1 MoJ has invested in a number of Information Managers (IMs) who were originally assigned responsibility for providing support to the implementation and users of TRIM. Broadening the remit of the network to encompass wider information management would support delivery of the KIM strategy and provide departments with the support they need to manage their information effectively. It is also recommended that the network is supported at a senior level within each business unit, to help ensure compliance with information management procedures.

**Recommendation 24: MoJ to review and refresh its IM network to help support good information management throughout MoJ HQ, in line with the KIM strategy.**

7.2 In NOMS a network of Local Information Managers (LIMS) assists the KIM function. LIMs are trained to provide advice and support on the use of corporate information systems, shared folders and the setting of access restrictions. However, many staff interviewed were unaware of this network. These roles need to function effectively and need the authority to do so. The support of the KIM team will enable consistency and ensure that KIM initiatives are translated across MoJ.

**Recommendation 25: KIM team to provide leadership and guidance to MoJ KIM specialists through creation of a support network.**

### Policies and Guidance

7.3 There is a wealth of information and guidance across both MoJ HQ and NOMS. The assessment team noted that KIM guidance was difficult to find on the intranet and that there was little or no communication about its existence. The team also noted that the guidance would shortly be out of date as a result of the circumstances surrounding TRIM, and would advise that it is refreshed as soon as possible.

**Recommendation 26: KIM team to ensure that the relevant polices and guidance are publicised.**

7.4 Prison Service Orders (PSOs) are the key guidance mechanism for the Prison Service, which are sent from the policy team within NOMS HQ. These cover all aspects of managing the prison services. The assessment team were advised that some prison governors actively take a PSO and translate this policy or guidance into succinct work instructions for their staff, while others view the PSOs as barriers to the work of the prison. As each prison governor has a level of autonomy, NOMS HQ requires annual compliance statements from each establishment on its implementation of PSOs. The LIM is responsible for coordinating this information. It may be appropriate for the NOMS policy team to assess some of these local work instructions to see if there is validity in sharing these across other prisons.

**Recommendation 27: NOMS to coordinate and share examples of local good practice.**

7.5 The assessment team found that understanding of protective marking systems was low in both MoJ HQ and NOMS, and that protective marking labels were inconsistently applied. This creates a significant risk that sensitive information will not be appropriately recognised or safeguarded.

7.6 In the probation service, by contrast, protective marking is well understood and consistently applied. The assessment team were impressed to learn that in some areas local initiatives had resulted in simple guidance for local use, which was accurate and comprehensible. The Shared Services Centre, for instance, has a ‘compliance passport’, awarded to staff after training in NOMS policies, data protection and protective marking. NOMS are currently developing a system to automatically assign protective marking to all emails. It is important that a single, authoritative set of central guidance be provided and is accessible to all staff. The application of the ‘compliance passport’ concept across the organisations might also be beneficial.

7.7 Work has continued on delivering coherent security policies for information.

**Recommendation 28: MoJ to ensure that central guidance is accessible, available and up to date.**

7.8 Across MoJ there is a reliance on contractors to deliver services. These contractors will have to handle large quantities of sometimes highly sensitive information. The end of year information assurance assessment includes reporting on delivery partner and third-party supplier compliance. All MoJ business groups were required to make an assessment of their suppliers information assurance compliance and report back to the centre. These third-party relationships are an integral part of modern government departments, and contractual arrangements for handling information need to be given as much close attention as those for service delivery.

**Recommendation 29: MoJ to instigate a review of its contract process to ensure that where possible the department's KIM requirements are included in third party contracts.**

**Training**

7.9 MoJ HQ has rolled out the Cabinet Office e-learning package to all staff on data handling and there was a general awareness of data security. However, the assessment team interviewed several staff that stated that they had not completed the training. This training is mandatory. MoJ needs to be assured that all staff have completed the training within a reasonable period. It is vital that staff manage and handle the vast amounts of both personal and sensitive information properly.

**Recommendation 30: MoJ to ensure that all staff access the refreshed e-learning data handling training and enforce compliance through personal development plans.**

**The Intranet**

7.10 Both MoJ and NOMS have separate intranet sites, both of which have been redeveloped quite recently. Most interviewees felt it had been improved. Records management guidance is clearly available on the

sites, although there is some duplication and broken links to external guidance.

**Recommendation 31: MoJ and NOMS to continue the work started on rationalising the content and cohesiveness of the intranet sites.**

## Culture

### Commitment

8.1 Both MoJ HQ and NOMS operate in a series of well-defined functional groups. Each directorate and division within those groups operates with a degree of independence reporting to a Director and then Director General. NOMS is an executive agency and is therefore expected to operate with its own management controls. MoJ and NOMS have begun to develop stronger links in relation to information management, for example in sharing best practice and through the use of shared policies and guidance. There is more that can be done to develop those links with a view to achieving greater efficiencies and making savings.

8.2 Staff in NOMS still have strong ties with the Home Office. For instance, the primary source of information about NOMS continues to be published on the Home Office website. Although this is no longer maintained, it is considered to be of continuing value. A lack of corporate identity can obstruct the effective use of information.

**Recommendation 32: MoJ to reinforce the importance of a value of a corporate identity across all its bodies as an adjunct to effective information management.**

### Staff Understanding

8.3 MoJ is committed to enabling the sharing of the appropriate information, with clear accountabilities. MoJ aspires to a culture where information sharing is the norm rather than being 'owned' by the divisions or even by individuals. This behaviour is often driven by a desire to avoid information being misinterpreted.

8.4 There is limited understanding among staff not directly involved with KIM of the value of information as an asset, of the importance of good quality management of those assets, and of the consequences of failure to manage them properly.

**Recommendation 33: MoJ to reinforce the benefits of sharing information across the organisation.**

### Knowledge Management/Transfer

8.5 There is insufficient knowledge transfer across MoJ, for instance in acquiring expert knowledge of staff before they leave. Similarly, there is no formal process for ensuring that knowledge is transferred from contractors and is preserved in files where it can readily be found. Knowledge transfer in a cost-saving environment is crucial to retaining the tacit information of the organisation.

**Recommendation 34: MoJ to establish a formal process to capture the tacit knowledge of staff and contractors as they leave.**

## 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 Management Assessment programme.

These recommendations, when agreed, will form an action plan that will be monitored.

| Business Area | Ref | Recommendation |
|---|---|---|
| Governance and Leadership | 1 | MoJ to demonstrate active and continual support of KIM at board level which is effectively distilled throughout the organisation. |
| | 2 | The KIM team to collate and share examples of good KIM practice across the department. |
| | 3 | MoJ to provide clear guidance on the use of corporate information management systems, ensuring that their use is part of internal governance processes. |
| | 4 | The KIM team to publicise its role to ensure that staff know who they should approach for help on KIM. |
| | 5 | MoJ to ensure that all relevant ICT projects include information management considerations, working in conjunction with the KIM team. |
| | 6 | MoJ to reassess the IM role to ensure they support the KIM agenda more effectively and their responsibilities are cascaded throughout the department. |
| | 7 | MoJ to continue to identify and publicise its information assets, raising awareness of their importance. |
| | 8 | NOMS to extend the definition of information risk to cover risks to the completeness, availability and usability of digital information. |
| Records Management | 9 | MoJ to implement a 'What to Keep' project, with the support of The National Archives, to implement 'What To Keep' guidance. |
| | 10 | MoJ to evaluate its options for corporate information storage, assessing its EDRM capability and the potential for more rigorously structured and monitored shared drives to meet its needs. |

| | | |
|---|---|---|
| | 11 | MoJ and NOMS to assess and mitigate the ongoing risk of managing and handling prisoner records from a number of sources. |
| | 12 | Staff must be instructed to store corporate information in the appropriate system. Technical controls should be considered to minimise the risks. |
| | 13 | The ICT function should work in partnership with KIM and business units to support good working practices, and ensure that technology meets requirements for the completeness and availability of information. |
| | 14 | MoJ should continue its programme of rationalising and consolidating the technology supporting the business. |
| | 15 | MoJ should continue to take active steps to phase out the use of duplicate systems and databases, decommissioning redundant technology. |
| | 16 | MoJ should ensure that ICT-enabled change projects conduct a formal impact assessment on the completeness and availability of information. |
| | 17 | MoJ to continue providing access to digital information as a key requirement for projects, expressed in terms of meeting business requirements for using this information. |
| | 18 | MoJ and NOMS to agree a process for managing risks to the continuity of digital records. |
| | 19 | MoJ and NOMS HQ to extend guidance on what information is critical to the business until a sustainable 'What To Keep' protocol is in place. |
| | 20 | NOMS to issue guidance for standards of data entry into Prison-NOMIS to enable consistency. |
| | 21 | MoJ to provide support and reinforce guidance on ensuring that operational and service information is complete and accurate. |
| Information legality | 22 | KIM team to reinforce guidance to staff on maintaining sensitive personal information. |
| | 23 | NOMS should give careful consideration to how it devolves responsibility for information assurance to local offices. |
| Compliance | 24 | MoJ to review and refresh its IM network to help support good information management throughout MoJ HQ, in line with the KIM strategy. |
| | 25 | KIM team to provide leadership and guidance to MoJ KIM specialists through creation of a support network. |
| | 26 | KIM team to ensure that the relevant polices and guidance are publicised. |
| | 27 | NOMS to coordinate and share examples of local good practice. |
| | 28 | MoJ to ensure that central guidance is accessible, available and up to date. |

| | | |
|---|---|---|
| | 29 | MoJ to instigate a review of its contract process to ensure that where possible the department's KIM requirements are included in third party contracts. |
| | 30 | MoJ to ensure that all staff access the refreshed e-learning data handling training and enforce compliance through personal development plans. |
| | 31 | MoJ and NOMS to continue the work started on rationalising the content and cohesiveness of the intranet sites. |
| Culture | 32 | MoJ to reinforce the importance of a value of a corporate identity across all its bodies as an adjunct to effective information management. |
| | 33 | MoJ to reinforce the benefits of sharing information across the organisation. |
| | 34 | MoJ to establish a formal process to capture the tacit knowledge of staff and contractors as they leave. |

APPENDIX TWO: GLOSSARY

| | |
|---|---|
| DPA | Data Protection Act |
| EDRMS | Electronic Document Records Management System |
| FOI | Freedom of Information |
| FOIA | Freedom of Information Act |
| HERM | HQ Electronic Records Management project |
| ICT | Information Communications Technology |
| IM | Information Manager |
| IMA | Information Management Assessment |
| KIM | Knowledge and Information Management |
| LIM | Local Information Manager |
| MoJ | Ministry of Justice |
| NOMS | National Offender Management Service |
| PSO | Prison Service Order |
| SIRO | Senior Information Risk Owner |
| TRIM | Tower Records and Information Management |