

# Information Management Assessment

---

Ministry of Justice

**Reviewed**

May 2016

**Published**

December 2016

Working with government  
to raise standards in  
information management

## Contents

	<b>Statement of commitment</b>	<b>02</b>
	<b>IMA background</b>	<b>02</b>
	<b>Glossary</b>	<b>04</b>
	<b>Key findings of the assessment</b>	<b>05</b>
	<b>Highlights table</b>	<b>14</b>
	<b>Recommendations to address risk areas</b>	<b>18</b>
<b>1</b>	<b>The value of information</b>	<b>22</b>
<b>2</b>	<b>Information and supporting technology</b>	<b>30</b>
<b>3</b>	<b>Information risk, governance and oversight</b>	<b>38</b>
<b>4</b>	<b>Records, review and transfer</b>	<b>49</b>

© Crown copyright 2016.



You may use and re-use the information featured in this report (not including logos) free of charge in any format or medium, under the terms of the [Open Government Licence v3.0](#).

Any enquiries regarding the use and re-use of this information resource should be sent to [psi@nationalarchives.gsi.gov.uk](mailto:psi@nationalarchives.gsi.gov.uk)

## Statement of commitment

The following statement was provided by the Permanent Secretary of the Ministry of Justice (MoJ). It is published on GOV.UK.

### **Statement affirming the Ministry of Justice commitment to The National Archives' Information Management Assessment programme.**

The Ministry of Justice Permanent Secretary Richard Heaton said:

'The Ministry of Justice last undertook an Information Management Assessment in 2010. This was part of the regular programme of assessments that The National Archives conducts to review information, records and knowledge management standards within government departments. To demonstrate the strength of the department's commitment I have asked The National Archives to carry out an Information Management reassessment in May 2016.

'The Ministry of Justice recognises the importance of meeting its corporate obligations to effectively manage, protect and exploit its information. The report that The National Archives produces will help me to support all aspects of knowledge and information management across the department. It will help to make sure that our information, knowledge and records are appropriately captured, managed and preserved, and information risks and sensitivities are suitably handled.'

### **IMA background**

The Ministry of Justice (MoJ) first underwent an Information Management Assessment (IMA) in June/July 2010. MoJ produced an IMA action plan that was signed off in July 2012 following the production of a formal progress report. The IMA report, action plan and progress review can be found on The National Archives' website at: [nationalarchives.gov.uk/information-management/our-services/imareports-action-plans.htm](http://nationalarchives.gov.uk/information-management/our-services/imareports-action-plans.htm)

MoJ committed to an IMA reassessment, which was conducted in May 2016. The MoJ IMA reassessment entailed a detailed review of supporting documentation, followed by interviews with senior staff including the Senior Information Risk Owner (SIRO), a Non Executive Board Member and Deputy Directors, knowledge and information management, information assurance and security and information technology specialists and practitioners and representatives from business areas in the department's London offices. These were conducted between 9 and 12 May 2016. The assessment focussed on MoJ headquarters (HQ) only. The following report provides a summary of good practice and risks identified.

# Glossary

**CIAB** – Central Information Assurance Branch

**DACU** – Data Access and Compliance Unit

**DPA** – Data Protection Act

**DRO** – Departmental Records Officer

**DROID** – Digital Record and Object Identifier, The National Archives' file profiling tool

**EDRM** – Electronic Document and Records Management

**ERM** – Electronic Records Management

**FOI** – Freedom of Information

**IA** – Information Assurance

**IA Co-ordinator** – Information Assurance Co-ordinator

**IA Lead** – Information Assurance Lead

**IAO** – Information Asset Owner

**ICO** - Information Commissioner's Office

**IICSA** – Independent Inquiry into Child Sexual Abuse

**IMA** – Information Management Assessment

**IMC** – Information Management Consultant

**Just Store** – Replacement for MoJ's current electronic records management system, TRIM

**KIM** – Knowledge and Information Management

**MoJ** – Ministry of Justice

**OSP** – Operational Selection Policy

**PSTs** – Personal Storage Tables, format used for storing email

**RMS** – Records Management Service

**RTR** – Records Transfer Report

**SIRO** – Senior Information Risk Owner

**SLAQ** – Series Level Appraisal Questionnaire

**TRIM** – MoJ's system for electronic records management

# Key findings of the assessment

## 1 The value of information

### Findings of the 2010 IMA:

There was a commitment to enabling better sharing of information across the Ministry of Justice (MoJ), and to building a greater understanding of the importance of Knowledge and Information Management (KIM) among staff and of the benefits it can bring.

Staff and teams frequently regarded corporate information as their own. MoJ needed to increase understanding across the department of the value of information as an asset and the risks of failing to manage those assets properly. MoJ also needed to establish consistency over the capture of knowledge of staff and contractors before departure.

MoJ had effective data protection, freedom of information and information assurance processes and policies in place. Staff at MoJ HQ demonstrated a thorough understanding of the Data Protection Act (DPA). However, good practice was not uniform and greater consistency in staff training on data protection was recommended, as was raising awareness of the risks under the Freedom of Information Act (FOIA) and DPA if the existence and whereabouts of information is unknown.

At the time of the IMA, MoJ was a leader in government on publishing information.

### Performance rating (2016 IMA reassessment)

**Communicating and realising value**

**Development area**

**Managing information as an asset**

**Satisfactory**

- There is evidence of senior support for knowledge and information management (KIM) at MoJ. With the roll-out of Just Store (a system to replace the current electronic records management [ERM] system, TRIM), there is a real opportunity for the Permanent Secretary and other senior staff to actively support and promote these activities. **See recommendations 1 and 2.**
- MoJ is in the process of drafting a new KIM strategy. The aim is to produce a two-year strategy with clear deliverables by Autumn 2016. The Head of KIM is also liaising with Digital Technology to ensure that it aligns with the digital strategy. MoJ should ensure that work on the strategy is completed and signed off at a senior level and that deliverables are included in the KIM and Records Management Service (RMS) business plans. **See recommendation 1.**
- MoJ needs to ensure that it has a process for reporting on progress against the KIM strategy to the senior team and that there is an opportunity for the team to challenge and interrogate progress. **See recommendation 1.**
- The Information Management Policy clearly sets out expectations of staff in terms of information and records management. MoJ would benefit from including more detail about the specific responsibilities of different staff. The policy will also need to be updated to reflect the move to Just Store and the roll-out of Microsoft Office 365. **See recommendation 4.**
- Generally, staff seemed to understand the importance of managing and protecting their information, but the extent to which they were acting on this was mixed, in part due to technical problems with TRIM (MoJ's current ERM system).
- MoJ has worked hard to address issues with timeliness of response to freedom of information (FOI) requests following monitoring by the Information Commissioner's Office (ICO) in 2015 and 2016. Figures have improved significantly (up to as high as 92%) and the Senior Information Risk Owner (SIRO) is working with the new Head of Information Operations on ongoing improvements.
- MoJ's approach to information asset management has improved significantly since the last IMA. There is clear and succinct guidance for staff on managing information assets that includes details on how to define an information asset. There is also a good template for Information Asset Registers (IAR), which includes information and records management aspects, such as retention.
- In practice, understanding of information assets among staff is still being

embedded. Ongoing training and communications will improve practice. For example, MoJ runs regular training for Information Asset Owners (IAO) and has been engaged with The National Archives' work on this. MoJ also ran a successful information security campaign from December 2016 to March 2016, which included posters throughout the building and in lifts in order to raise awareness. **See recommendation 3.**

- There are a number of roles within MoJ that have responsibility for the management of information assets, including IAOs, Information Assurance Leads and Information Assurance Co-ordinators. The roles are defined but it is clear there is some overlap between them and it is not necessarily easy for staff to understand how they fit together in practice. MoJ should increase staff awareness of the existence and purpose of these roles. It may benefit from reviewing and potentially streamlining the number of roles involved as part of a wider review of security and information governance which is planned in response to the Transforming Government Security review. **See recommendation 3.**



## 2 Digital information and supporting technology

### Findings of the 2010 IMA:

MoJ created vast amounts of information, which was stored in numerous legacy and bespoke systems across different platforms and formats. The systems were often perceived to be unstable, unreliable and difficult to use by staff.

The lack of a fully-utilised corporate information system and the inability to technically share information across MoJ represented an obstacle to free sharing of information. TRIM was unsupported, but to upgrade to a new version would be prohibitively expensive. MoJ also needed to review its ERM provision and manage negative staff perceptions of systems for storage of information.

### Performance rating (2016 IMA reassessment)

**Supporting information through technology**

**Development area**

**Digital continuity and IT change**

**Development area**

- TRIM has enabled MoJ to manage records throughout its lifecycle in line with the section 46 code of practice on the management of records. However, it has not been upgraded since the last IMA and there have been a number of technical issues with TRIM following the move to Windows 8, making it difficult to save emails and documents. In addition, TRIM does not work well remotely.
- MoJ is moving to a new electronic records management system – Just Store (SharePoint 2013 with Automated Intelligence plug-ins) – to address the issues above. The KIM team, in particular, has done good work around preparing to bring in Just Store, which will have full lifecycle capability and bring further benefits around collaborative working. The project has been delayed due to the MoJ spending review in 2015 but roll-out is due to start imminently to around 3,000 users.

- Microsoft Office 365 is also being introduced across MoJ. Implementation starts in the autumn and will take around 18 months. This will be rolled out to 37,000 users across the whole of the department, not just to MoJ HQ. Office 365 will bring with it a range of tools that do not support the lifecycle management of information: as a result, this may undermine the success of Just Store if staff choose to use these tools instead. Communications, policy, guidance and training will help mitigate this risk and MoJ should look at the experience of the Houses of Parliament in bringing in Office 365. **See recommendation 4.**
- Enterprise Vault is in place for email: there is a clear policy that this is just for back up purposes and record emails need to be saved in TRIM or shared drives. Staff do not always follow this policy and, in addition, no disposal is applied to Vault at the moment. MoJ needs to apply disposal to Vault in order to avoid a huge build-up of email and to incentivise staff to save emails to TRIM/Just Store. **See recommendation 4.**
- MoJ has a large amount of information on shared drives that is not currently subject to any central oversight or control and this poses significant compliance and business risks. MoJ needs to develop a plan for moving away from the shared drives. In order to maximise take-up of Just Store it should consider restricting access to shared drives following roll out. MoJ would benefit from exploring the Department of Business Innovation and Skills' approach. **See recommendation 4.**
- There has been a noticeable improvement in the cooperation between KIM/Records Management Services (RMS) and IT since the last IMA in 2010. Continued communication and collaboration on projects such as Just Store and Office 365 and work around the KIM strategy should help to improve this further. **See recommendations 1 and 4.**
- MoJ has made progress since the IMA in building digital continuity considerations into business-as-usual processes. For example, digital continuity is included as part of its information asset and risk management processes.

### 3 Information risk, governance and oversight

#### Findings of the 2010 IMA:

MoJ had prepared the ground for effective corporate structures to manage its information. It had established robust policy and guidance frameworks and was taking steps to tackle the many information management challenges facing the department. However, many of the business areas assessed did not adhere to the policy requirements, leading to local practices and a lack of consistency. More join-up was needed between KIM and IT and more Board level support was recommended.

MoJ had recently revised much of its information management guidance, although it was not always easily accessible. MoJ needed to improve the guidance, particularly on what to keep and knowledge capture. There were a number of specialist KIM roles in place across the organisation that could be used to manage information more effectively. While figures indicated that all staff had completed the mandatory Cabinet Office e-learning package on Information Assurance, it was evident that understanding of data security issues could be better in some areas.

#### Performance rating (2016 IMA reassessment)

<b>Recognising information risk</b>	<b>Good practice</b>
<b>Establishing control</b>	<b>Satisfactory</b>
<b>Providing guidance</b>	<b>Good practice</b>
<b>Measuring Impact</b>	<b>Development area</b>

- MoJ has a good framework in place for managing information risk. The SIRO Board and IA Leads Committee play a key role in the risk management process and the overall structure and process provides a good level of scrutiny.

- Understanding of information risk has improved and further training, guidance and communications will continue to embed this. **See recommendation 3.**
- Risks on information management and digital continuity are included on the SIRO Board Risk register and appropriate mitigating actions are listed. MoJ should also include risks around cyber security and reflect the impact of IT change here or elsewhere within in its risk framework. **See recommendation 3.**
- The KIM and RMS teams are providing a good service to the business and there were many positive comments about their work. There is liaison on areas such as retention and disposal scheduling, what to keep, and recalling paper files. The KIM team also provides support around knowledge management, use of TRIM and preparation for Just Store roll-out. Staff commented that they could get the support they needed.
- MoJ has an established network of Information Managers in business areas who support colleagues on information and records management. They will play a crucial role in the Just Store roll-out. There are regular forums for Information Managers and also a regular newsletter. As MoJ moves to Just Store it should check that Information Managers have the right skills to support staff in this. **See recommendation 4.**
- The KIM team has recently reviewed and revitalised the Knowledge Champions network. The Champion roles aim to reinforce the importance of information and records management. The role is meant to be held at Senior Civil Service (SCS) level, although in practice this has often been delegated to Grade 7 or below. **See recommendation 2.**
- MoJ has produced a comprehensive set of guidance covering all aspects of information and records management that is clear and succinct and is available on the intranet. It also provides bespoke training for business areas on this. A full programme of training is planned to accompany the Just Store roll-out.
- MoJ has significantly improved its approach to knowledge management, including adoption of the 'Head Start' form and 'an audience with' sessions for capturing knowledge. With a Voluntary Exit Scheme soon to take place, there

needs to be an increased focus on knowledge transfer in the coming months.

**See recommendation 2.**

- As yet there is no system for measuring compliance with information and records management policy in the business. MoJ would benefit from developing a monitoring process and should explore the work that HM Treasury and Home Office have done here. **See recommendation 5.**

#### 4 Records, review and transfer

##### Findings of the 2010 IMA:

Defined criteria were not consistently being applied to digital and paper files to ensure that information that should be retained was not being destroyed. In a number of areas this was due to time pressure. In other areas, local or individual criteria were being applied.

##### Performance rating (2016 IMA reassessment)

Oversight of records and selection	Satisfactory
Implementing disposal decisions	Satisfactory

- The Departmental Records Officer (DRO) and her team are fulfilling all aspects of the role as detailed in The National Archives' guidance. The Records Management Service works very closely with the KIM team and the DRO and Head of KIM have a good working relationship. The DRO sits also on the SIRO Board.
- MoJ is currently ahead in its transition to the 20-year rule, as demonstrated by Records Transfer Report figures. However, the volume of paper files doubled between 1992 and 1996 so MoJ will need to start looking for ways to speed up the paper appraisal process in order to keep pace with the transition to the 20-year rule. **See recommendation 6.**
- MoJ has made major inroads into developing a process for review of digital records. It has carried out appraisal for records on TRIM up to 2014 and around

5,000 files are marked for preservation. MoJ has also done some exploratory work regarding sensitivity review (MoJ was a pilot department for The National Archives' Digital Transfer Project). There is no process yet in place for applying this to the shared drives and MoJ needs to address this. The RMS team is aware that it will need tools to help assist with sensitivity review but cost is an issue here – it would be useful to look at what other government departments and The National Archives are doing around this. **See recommendation 6.**

- MoJ has developed and maintained its retention schedules and its what-to-keep policy and guidance since the last IMA. MoJ has a clear idea of what needs to be kept and how long for, and has applied disposal to TRIM. Staff would benefit from a renewed focus on this as Just Store is rolled out. Disposal is largely on hold due to the requirements of the Independent Inquiry into Child Sexual Abuse (IICSA). What-to-keep and disposal guidance and schedules have been updated to reflect these requirements. Disposal has not yet been formally applied to the shared drives and this needs to be addressed. **See recommendation 6.**

## Highlights table

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

### Highlights of the 2016 IMA reassessment

The Ministry of Justice (MoJ) has produced clear and succinct guidance on information assets. The Information Asset Owner (IAO) Handbook is comprehensive and covers the IAO role, training, information assets, access, risk management and other statutory requirements. It includes a definition of an information asset (which covers value, content and records management), advice on how to identify them and some examples of potential assets. The guidance goes well beyond purely defining information assets at a systems level, stating that an information asset can be: 'a single significant record/document or a set of related data, documents or files. It can be shared or be confined to a specified purpose or organisational unit.'

MoJ has produced a good template for its Information Asset Registers and this is available centrally. IARs are expected to be completed and maintained locally, mostly at Director or Deputy Director level in MoJ HQ. A column on the IAR has been included to record retention periods, data sharing agreements, technical risk management and digital continuity. On the latter point MoJ and The National Archives ran a workshop in 2014 with IA Leads to decide how to incorporate digital continuity considerations into the IAR.

MoJ has made good progress in ensuring that information risks are recognised and managed corporately. The SIRO Board Risk Register for February 2016 includes information risks on digital continuity and legacy systems and there are appropriate mitigating actions listed for these.

There is a good framework in place for managing risk within MoJ and information risks are included as part of this. The SIRO Board and IA Leads Committee provide an opportunity for information risks to be discussed and scrutinised.

MoJ has an established network of Information Managers. Their responsibilities are clearly defined and are to ensure that digital records are structured and managed appropriately in their business area and to provide support to colleagues in managing digital records. Skills required for the role include good IT skills and a willingness to learn, a good knowledge of business functions in their area, ability to communicate and influence and advise on records and information management.

The KIM team oversees the Information Managers, providing training and guidance as required. There is an Information Managers' forum that meets quarterly and which provides an opportunity to communicate important messages as well as discuss issues and share best practice. The KIM team also sends out a monthly IM newsletter via email. Information Managers will play a crucial role in the Just Store roll-out.

MoJ has recently updated its process and guidance for knowledge management, which marks a major step forward since the last IMA. The knowledge management page on the intranet has been rewritten and new guidance around knowledge capture/handover, including a head start form and guidance and a leaver's checklist, has been produced. This was about to



be signposted as part of the knowledge management campaign that MoJ has been running. MoJ has also developed 'an audience with' sessions for senior people or for specialists in their field in order to capture knowledge before they leave and give colleagues a chance to ask questions. Sessions were held last year when around 80 technology staff left MoJ.

Also of note is the information security campaign that MoJ ran from December 2015 to March 2016, which aimed to increase staff awareness and understanding of their responsibilities when handling departmental information. Activities included drop-in sessions, articles, emails and poster campaigns. Each month had its own theme and issues such as safe remote working, cyber security and good information handling were covered. The impact of the campaign was tested through surveys, test phishing emails, statistics on who attended events or read intranet articles and the number of people who completed the Responsible for Information e-learning.

MoJ has developed a high-level policy on what to keep and each business area has a retention schedule. There are over 95 record retention and disposition schedules that govern the departmental records. These cover all types of records and state when they can be either selected for destruction or kept for review after 20 years. MoJ has published these in line with Sir Alex Allan's recommendation in his Report on Records Review.

MoJ also has an Information Review and Disposal Policy that links in with the above. The what-to-keep guidance is clear, succinct and easy to read. The retention schedules are developed and updated in conjunction with business areas to ensure that these work in practice and the right information is kept to enable business areas to carry out their work.

MoJ has developed a process for appraisal and selection of digital records on TRIM (MoJ's system for electronic records management). Work on this began in 2014. File by file review was tested but proved to be too labour-intensive for digital records, so MoJ is taking a macro approach to reviewing at level 3 in TRIM. Once records have been identified for selection, the file path is exported from TRIM onto a spreadsheet and review comments are added. The National Archives' IMC has access to a TRIM account and can access the spreadsheet to make comments and sign off decisions. MoJ have reviewed records in TRIM up to 2014 and around 5,000 folders have been identified and marked for transfer to The National Archives. These records will be migrated to Just Store (the electronic records management system to replace TRIM) along with the rest of the records in TRIM and will be transferred to The National Archives in due course from there. (They are not due for transfer until 2022). There will be a records center for each year of selected material transferred to Just Store. The same approach to appraisal and selection will be applied to new records created in Just Store.

## Recommendations to address risk areas

### Recommendation 1

**The Ministry of Justice (MoJ) should ensure that it has established clear and integrated goals for knowledge and information management.**

This would be supported by:

- completing work on the Knowledge and Information Management (KIM) Strategy and ensuring this is signed off at a senior level
- getting senior support for the strategy – for example, asking the Permanent Secretary to provide a foreword
- continuing to liaise with Digital Technology to ensure that strategies are aligned
- including deliverables from the strategy in the KIM and Records Management Service (RMS) business plans
- ensuring that there is a process for reporting on implementation to the senior team and an opportunity for the team to scrutinise progress, via the SIRO Board

### Recommendation 2

**MoJ should actively work to improve its culture of knowledge, information and records management.**

This would be supported by:

- senior staff actively supporting and promoting KIM activities – for example by providing a foreword for the KIM Strategy, speaking at KIM events or blogging
- ensuring that the Knowledge Champion role is not delegated below Senior Civil Service (SCS) level
- Knowledge Champions proactively promoting messages around knowledge, information and records management and ensuring that staff are complying with policy
- including more detail in the Information Management Policy on specific responsibilities of staff at all levels, but particularly middle management; the

Northern Ireland Office and Houses of Parliament Information Management Policies are good examples

- providing a method of monitoring compliance with information and records management policy using a maturity model and introducing an element of competition between business areas (see also recommendation 5)
- increasing focus on knowledge transfer in the coming months because of the Voluntary Exit Scheme
- maintaining improvements in FOI performance and updating its publication scheme
- continuing to proactively identify information that can be published and improving its openness score by publishing datasets in a more usable format.

### Recommendation 3

**MoJ should continue to embed its process for information asset management and information risk.**

This would be supported by:

- continuing to improve understanding of information assets through guidance, training and responsible roles such as Information Asset Owners (IAO) and Information Assurance Leads (IA Leads)
- increasing awareness of the existence and purpose of the various roles, such as IAOs, IA Leads and Information Assurance Co-ordinators, through communications, guidance and training
- reviewing and potentially streamlining the number of roles involved in the assurance process as part of a wider review of security and information governance which is planned in response to the Transforming Government Security review
- ensuring that there is no conflict of interest when staff carry out dual roles such as group level Senior Information Risk Owner (SIRO) and IAO
- including risks around cyber security on the SIRO Board Risk Register or elsewhere in MoJ's risk framework and ensuring that it reflects the impact of IT change
- including mitigating actions on the role of Knowledge Champions and in promoting policy and compliance.

## Recommendation 4

**MoJ should continue to ensure that it has a technology environment that supports the management, protection and exploitation of information and that this is used effectively by staff.**

This would be supported by:

- addressing the risk of staff not using Just Store (the replacement for the TRIM electronic records management system) through training, guidance and highlighting benefits of use to staff
- continuing to work collaboratively with Digital Technology, in particular on work around Just Store, Microsoft Office 365 and future plans for shared drives
- ensuring that roll-out of Microsoft Office 365 does not undermine use of Just Store through communications, policy, guidance and training
- examining the experience of the Houses of Parliament in rolling out Microsoft Office 365 and in working to address the issues
- as part of considerations around the future approach to shared drives, MoJ ensuring that work is included to make information held there more discoverable as well as considering how it will better control access
- acquiring DROID to get an overall sense of what is on shared drives and help to identify duplicates
- restricting access to shared drives once Just Store has been rolled out to maximise its use
- exploring the work that the Department for Business Innovation and Skills has done on moving away from shared drives
- encouraging staff to save emails of value into corporate systems
- putting plans in place to dispose from Enterprise Vault (bearing in mind the requirements of the Independent Inquiry into Child Sexual Abuse) and draw on the experience of Welsh Government
- Knowledge Champions and Information Managers encouraging staff to follow policy around email and personal drives, and ensuring that they do so
- ensuring that Information Managers have the right skills to support staff in the move to Just Store
- updating the Information Management Policy and other policy and guidance to reflect the roll-out to Just Store
- reminding staff of what-to-keep policy and related guidance.

### Recommendation 5

**MoJ should explore how it can better monitor compliance with knowledge and information management policy.**

This would be supported by:

- exploring the work that Home Office and HMT Treasury have done to monitor compliance through their One3M and the Knowledge Management Benchmarking processes
- drawing up a maturity model and developing a process to monitor business areas against this
- considering how Information Managers and Knowledge Champions can play a role in any compliance monitoring process.

### Recommendation 6

**MoJ should build on the good work it has already done in developing a successful approach to the appraisal, selection, sensitivity review and transfer of its paper and digital records.**

This would be supported by:

- exploring ways of speeding up the process of paper review, using macro methods where possible, in order to keep pace with the transition to the 20-year rule
- developing a process for appraisal, selection, sensitivity review and transfer of digital records on the shared drives
- using the experience of developing a process for the appraisal and selection of records on TRIM (MoJ's electronic records management system) to inform work on shared drives
- applying disposal to the shared drives
- continuing to participate in the work that The National Archives and other departments are doing in this area
- considering the possibility of joining with other departments to share a solution for sensitivity review
- acquiring DROID (The National Archives' file profiling tool) to help gain an overview of the information on the shared drives and to enable digital transfer.

# 1 The value of information

## 1.1 Communicating and realising value

Goal: The organisation establishes information's value in principle and supports its realisation in practice.

### Establishing the importance of information

We saw evidence of senior management support for and engagement with information and records management within the Ministry of Justice (MoJ). The former Permanent Secretary's statement of commitment on the IMA was published on GOV.UK, publicly demonstrating his commitment to the process. The current Permanent Secretary, Richard Heaton, has been driving work to improve MoJ's Freedom of Information (FOI) performance along with the Senior Information Risk Owner (SIRO). He has also attended the SIRO Board and a recent Hackathon event. With the roll-out of Microsoft Office 365 and Just Store (MoJ's replacement for its TRIM system for electronic records management) and work on a new Knowledge and Information Management (KIM) strategy, there is a real opportunity for the Permanent Secretary and other senior staff to actively support and promote MoJ's vision for its information, for example by providing a foreword for any new KIM strategy, speaking at launch events and blogging. **See recommendations 1 and 2.**

There was also evidence that information and records management issues are being discussed within business areas and by managers. For example, one Information Asset Owner (IAO) stated that TRIM, email etiquette and retention issues had all been discussed at weekly meetings. Another interviewee recalled 'discussing email usage with their team and the possibility of cutting down on unnecessary email traffic'. The Knowledge Champion role is potentially a very useful way of getting Deputy Directors more engaged with information management. It is expected that Knowledge Champions will play an important role in promoting good practice and the effective use of Just Store as roll-out begins. However, the role has occasionally been delegated. This practice should be discouraged and the KIM team should

check that the Knowledge Champion role is appointed at an appropriate senior level in business areas. **See recommendation 2.**

The MoJ Information Management Policy was updated in March 2016. It clearly sets out staff responsibilities in managing information within corporate systems. For example, it states that:

‘Information that has any interest or evidential value to others in the team or wider department must be stored in a shared electronic information storage area so that it is available to others. This may be TRIM or a shared drive. All electronic records must be stored in TRIM, the MoJ’s Electronic Document Records Management (EDRM) system.’

However, MoJ would benefit from including more in the policy about the specific responsibilities of staff at all levels, but particularly middle management. It would be useful to look at the Northern Ireland Office and Houses of Parliament Information Management Policies which cover this effectively. The policy will also need to be updated to reflect the move to Just Store and the roll-out of Microsoft Office 365. **See recommendation 4.**

KIM messages are largely communicated via the intranet, policy, guidance and training: MoJ has also held recent communication campaigns on information security and knowledge management (see section 3). The poster spaces in the lifts at Petty France are used to promote messages on information and records management and information security. Information Managers in business areas also play an important role in promoting good information and records management practice.

Generally, staff seem to understand the importance of managing and protecting their information, but the extent to which they are acting on this is mixed. The recent problems with TRIM (see section 2.1) have not helped, though there are examples of staff still striving to the right thing in spite of this. Also, the continuing availability of shared drives means there is the ability to store records outside the corporate



system, though there was evidence that some teams had made an active decision not to use these and to put their records in TRIM instead.

### **Setting goals for information and its management**

A KIM Strategy is in development. A draft was not provided as part of the evidence for the IMA but we were told that the aim is for it to be 'brief, snappy and tightly-focused.' Given the amount of change happening in MoJ at the moment it is likely to be a short, two-year strategy with well-defined deliverables, to avoid it becoming quickly outdated. There was a recognition that the cultural aspects (how an organisation can develop a good culture of information records and encourage staff towards managing their information and records in the right way) are very important, particularly as MoJ moves to Just Store and Microsoft Office 365, and that this should form a core part of any KIM strategy. One interviewee felt that Just Store should not just be sold as a repository but also as something that will make people's lives easier if the system is used properly: 'More emphasis is needed on preparation for Just Store – we don't want TRIM all over again. There needs to be a culture change driven by a carrot and stick approach.' The Head of KIM has already spoken to The National Archives about the Cross Government Digital Records Management work on behavioural change. MoJ should ensure that work on the strategy is completed and signed off at a senior level and that deliverables are included in the KIM and RMS business plans. **See recommendation 1.**

The Digital and Technology Directorate (Digital Technology) has a strategy that it is in the process of refreshing. It will also be refreshing the digital 'transformation' strategy following a commitment to the Government Digital Service (GDS) that it will refresh its digital strategy by September. The KIM Strategy needs to align with this work and any IT strategy needs to link to the KIM Strategy. At the time of the IMA, the Head of KIM was planning to meet with colleagues in Digital Technology to discuss this. **See recommendation 1.**

## **Enabling public access to information and supporting transparency and re-use**

Freedom of Information (FOI) performance up to end of 2015 had been poor. MoJ received 4,034 FOI requests overall in 2015 – the second highest amount among departments of state. Of these requests, 73% were met the 20-day deadline and 74% were answered ‘in time’ (i.e. meeting deadline or within a permitted extension). This is well below the minimum level of 85% set by the ICO, below which monitoring may take place. Figures reached a low of 65% in quarter 3. The ICO initially monitored MoJ’s performance between September and November 2015. This period was then extended to March 2016.

By the end of the monitoring period, monthly performance had reportedly improved to 92%. Senior staff appeared to have played a significant role in driving this, with the Permanent Secretary, the Senior Information Risk Owner (SIRO) and Director of Communications and Information active and engaged in driving ongoing improvements. One senior interviewee stated: ‘The profile of FOI is high and senior involvement has had an impact. I see weekly statistics and Deputy Directors are expected to account for any delays.’ MoJ has not, up to now, had a system for tracking its FOI requests. However, there is a project to put in place a system for tracking FOI, which should improve performance. MoJ should work to ensure that this improvement continues. **See recommendation 2.**

MoJ has a partially up-to-date publication scheme. Due to resourcing issues over the last 12 months, it has not been updated as regularly as it should have been. MoJ hopes to tackle this issue in the coming months. **See recommendation 2.**

As of 4 May 2016, MoJ had published 196 datasets on data.gov.uk and had received a total of 66 stars. MoJ received only an average score of 0.4 for openness – largely due to the fact that some of the datasets had been published in HTML format. There were 1,369 publications by MoJ on GOV.UK, 152 of which were transparency data. MoJ should continue to proactively identify information that can be published and improve its openness score by publishing datasets in a more usable format. **See recommendation 2.**

## 1.2 Managing information as a valued asset

Goal: The organisation protects, manages and exploits its information assets to achieve maximum value.

### Defining and cataloguing information assets

MoJ has produced clear and succinct guidance on the management of information assets. The Information Asset Owner (IAO) Handbook is comprehensive and covers the IAO role, training, information assets, access, risk management and other statutory requirements. It includes a definition of an information asset (which covers value, content and records management) and provides practical examples of potential assets. The guidance goes well beyond purely defining information assets at a systems level, stating: 'An information asset can be 'a single significant record/document or a set of related data, documents or files. It can be shared or be confined to a specified purpose or organisational unit.' **This is good practice.**

MoJ provides a central Information Asset Register (IAR) template and guidance. IARs are expected to be completed and maintained locally mostly at Director or Deputy Director level at MoJ HQ. A column on the IAR has been included to record retention periods, data sharing agreements, technical risk management and digital continuity. On the latter point, The National Archives provided Digital Continuity training in 2014 to IA Leads at a workshop to decide how to incorporate this into the IAR. **This is good practice.** The completed IAR we viewed was populated well, although it was unclear how well the template was being used across the rest of the organisation.

Understanding of information assets is still embedding across MoJ. For example, some staff still think it means datasets or personal information rather than the wider definition described above. MoJ should continue to improve understanding of information assets through the guidance, training and responsible roles. **See recommendation 3.**

The KIM team works closely with the Central Information Assurance Branch (CIAB). It is based in the same business area and sits in the same office. The Head of CIAB also took over responsibility for KIM for around a year in 2014-15. This has helped to build a good working relationship between the two teams and a shared understanding of how information assurance and information and records management fit together. **This is good practice.**

### **Ownership of information assets**

MoJ has a good structure in place for the management of information assets and there are a number of roles that have responsibility for this. Group-level SIROs are supported by Information Assurance Leads (IA Leads) and Information Asset Owners (IAOs), with Information Assurance Co-ordinators at directorate level. Some interviewees felt that this was quite a complex structure and did not always fully understand what all these roles are for or how they fit together (see also section 3.1). MoJ should increase awareness of the existence and purpose of these roles through communications and guidance. It may also benefit from reviewing and potentially streamlining the number of roles involved as part of a wider review of security and information governance which is planned in response to the Transforming Government Security review. **See recommendation 3.**

IAOs are largely at Director or Deputy Director level. The MoJ IAO handbook states that IAOs should be 'senior individuals', which is in line with the Security Policy Framework, although there was some feeling that Deputy Directors are expected to be IAOs as a matter of course. IAOs are responsible for the day-to-day use and risk management of their information assets, as well as supporting their SIROs in carrying out their duties. They are also responsible for identifying and managing the risks associated with their information assets as well as ensuring that staff have received appropriate training and understand their responsibilities for keeping information secure. All IAOs are expected to attend an MoJ IAO workshop run by the CIAB. A total of 286 IAOs, including those within IA support roles, were trained between 2013 and March 2016.

MoJ recognises information asset governance as a key element of its information assurance obligations. IA Leads are the main contacts on Information Assurance (IA) issues for business groups. They support their SIROs and assist in ensuring that good IA practice is followed within their business areas. In addition, they assist IA Co-ordinators and IAOs in their business areas to complete and maintain information asset registers, and to manage information risks, as well as ensuring that all staff are aware of their IA responsibilities and complete information risk training annually.

IA Co-ordinators are the first point of contact for IA issues at HQ directorate level. They provide local information for the HQ Business Group IA Lead and assist their IAOs and colleagues with the day-to-day implementation of appropriate and effective IA controls, including maintaining the Information Assurance Asset Register, risk assessments and the annual assurance statement for their SIROs.

The IAOs and IA Leads we spoke to were generally aware of what their responsibilities are and take their role seriously. All appear to be working to understand their obligations, with one noting that a good handover had been received with a group level briefing on their role available. They were aware of and had taken advantage of the guidance. We saw positive indications from IAOs and other interviewees that the provision of assurance by IAOs was taken seriously and that IAOs were challenging/querying context they received as part of the annual reporting process. However, at least one of the IAOs we interviewed was also acting as SIRO for their Group, which potentially means they would be signing off on their own assurance. **See recommendation 3.**

MoJ has been very engaged with The National Archives' work on information assurance and risk. The National Archives ran a number of bespoke train the trainer sessions for MoJ staff in October and December 2015 and March 2016. The IAO Workshops have been running in-house since November 2015. These workshops have been continued to be run very successfully by the CIAB team since April 2016 and the team continue to engage with TNA to ensure their approach is robust and guidance and briefing materials are comprehensive and up-to-date. MoJ plan to continue this work and plans are in place to increase the number of staff trained in

delivering the training and to maintain a pool of presenters and trainers for the workshops. **This is good practice.**

## 2 Information and supporting technology

### 2.1 The technology environment

Goal: The technology environment supports the management, protection and exploitation of information.

#### Corporate storage of information

The Ministry of Justice (MoJ) currently uses TRIM EDRM software version 5.2.4 – which is over ten years old – as its electronic records management (ERM) system. TRIM has enabled MoJ to manage records throughout their lifecycle, including disposal, and supports Section 46 requirements for storage of information. The move to Windows 8 has impacted on the functionality of TRIM and it has become more difficult for users to save emails and documents into the system. For example, TRIM icons no longer appear in the Outlook email system and staff are required to save emails to a personal drive first before moving them into TRIM. There has been a drop in how much is being saved to TRIM: the KIM team would normally expect a figure of around 11GB per month and this has dropped to 9GB, a small but not insignificant decline.

A decision was taken not to address these issues as MoJ is about to move to a new ERM system, Just Store (see below). There is a risk that important records are being stored outside TRIM and MoJ needs to ensure that staff are encouraged to move important documents/emails from personal drives to Just Store as it is rolled out to them. By the time Just Store has been rolled out, there is also a risk that staff may have got out of the habit of using an ERM system, preferring to save on personal or shared drives. This risk should be addressed through the communications, guidance and training that will accompany the Just Store roll-out. As part of this, MoJ should highlight the benefits for staff of using Just Store. For example, according to the KIM team, training for Information Managers will cover why using Just Store is important and the benefits of doing so as well as the technical side. **See recommendation 4.**

Roll-out of a new ERM system to replace TRIM, Just Store (SharePoint 2013 with Automated Intelligence Compliance Extender and SyncPoint to facilitate records management and email connection), has been delayed as all technology projects were paused during the MoJ spending review in 2015. MoJ plans to start the roll-out in July 2016 and hopes that staff will have access to it by November 2016. As a result of budget limitations it will not be available to all in MoJ HQ but will be rolled out to around 3,000 staff. MoJ prepared detailed recommendations prior to going out to tender for this and carried out a review of the requirements of individual business areas to identify which had the most important information and were most in need of an ERM system.

The KIM team has done a lot of good work in preparing to bring in Just Store, which will have full lifecycle capability and bring further benefits around collaborative working. Detailed business requirements for information and records management were prepared prior to the invitation to tender and procurement exercise. Responses were carefully examined against these requirements. Following the selection of a SharePoint-based solution, the KIM team has worked alongside the business and technical partners to build the Just Store system. Governance of the Just Store project is slightly unusual in that Digital Technology controls the budget (Digi Tech agreed to fund the project as a solution to the issue of TRIM), but the KIM team is the figurehead for the project. However, the arrangement between KIM and Digital Technology is working at the moment.

In addition to the roll-out of Just Store, Digital Technology is leading on a project to bring in Microsoft Office 365. Roll-out starts in the autumn and will take around 18 months. This is a much bigger project than Just Store and covers around 37,000 users right across MoJ, not just HQ. Office 365 will bring with it a range of tools that do not support the lifecycle management of information as outlined in the Section 46 Code of Practice. For example, there could be a second instance of SharePoint and other tools such as One Drive that staff may use instead of Just Store. This may undermine take-up of and the success of Just Store. Communications, policy, guidance and training, including a clear message on what the various different tools should be used for, will help mitigate this risk. MoJ would also benefit from looking at



the experience of Parliament regarding its Office 365 roll-out and how it is working to address the issues. **See recommendation 4.**

Shared drives are also in use alongside TRIM and, although not all business areas use them, a large amount of information is held here. One interviewee noted: 'Some teams are relying on shared drives. There was a threat a few years ago to freeze them, but that never happened.' Staff responsibilities for records management when using the shared drives are covered in the Information Management Policy.

However, information on the shared drives is not subject to any technical controls to enable records management rules and only a small proportion is structured according to corporate functions. To apply records management rules to the shared drives would require a significant investment in technology to support review and disposal. It poses serious compliance risks in relation to Data Protection and FOI as well as digital continuity, IT capacity, and storage costs. The Future Information Technology Solutions (FITS) Programme is looking at future management of the shared drives and MoJ needs to have a plan for moving away from these. In order to maximise take-up of Just Store, MoJ should consider restricting access to shared drives once the roll-out is complete. MoJ would benefit from exploring the work that the Department of Business, Innovation and Skills has done on this. **See recommendation 4.**

Staff also have access to personal drives and these are currently being used as part of a workaround for saving emails and documents to TRIM. Although staff we interviewed generally did not use personal drives to store corporate information, it is likely that usage of these will increase, given the technical issues with TRIM (see above).

As mentioned earlier, Outlook connects to TRIM, although technical issues mean that it is no longer possible to save emails directly to TRIM (see above). Emails are therefore not always being saved into TRIM or shared drives and some interviewees admitted to using Personal Storage Tables (PSTs) to store emails, even though there is very clear policy and guidance in place around email management. All record-worthy emails should be saved into a shared electronic storage area to

enable them to be shared and managed appropriately. This is particularly important with a number of staff due to leave in the Voluntary Exit Scheme, later in 2016. **See recommendation 4.**

Enterprise Vault is also used for email (although not by all staff) and there is a clear policy that this is just for back-up: record emails need to be saved in TRIM or shared drives. However, we saw evidence that not all staff are following this policy. One interviewee stated: 'In some ways, email Vault is handy because you don't have to worry about running out of space if you don't put things in TRIM.' Another said: 'Often email just gets archived and then it's the usual thing of trying to identify things when you move teams.' Where Vault is in place, emails are automatically archived based on age and mailbox quota. When the archiving task runs it will first check to see which items are over 30 days old and archive them. It will then check to see if the mailbox is under quota; if it is not, it will continue to archive more emails, but will never archive emails younger than seven days. However, no disposal is applied to Vault at the moment. MoJ will need to apply disposal in order to avoid a huge build-up of email and to incentivise staff to save emails to TRIM and/or Just Store. MoJ would benefit from drawing on the experience of Welsh Government on managing an email archive and tackling staff reliance on email. **See recommendation 4.**

Yammer and Trello are also used for collaboration purposes within MoJ. There is guidance in place around the use of these types of systems: the guidance highlights security aspects and that records need to be saved in TRIM or shared drives, particularly those that might be of historical value and should be transferred to The National Archives for permanent preservation.

### **Finding, accessing and protecting information**

Technical difficulties have made it more difficult to access information within TRIM when working off site. The TW3 project at MoJ has introduced new hardware and encourages remote working. However, TRIM does not work well remotely at present, making it difficult for staff to access information held there when they are working out of the office. One interviewee said: 'Remote working makes the system almost

unusable. It can take several minutes until something is saved. It's seriously disruptive and can end up losing all edits.' Another stated: 'You may be ok saving a small document early or late in the day, but if you are trying to save something in the middle of the day you are likely to really struggle. It can take so long – and in the meantime you can't do anything else. Your system is locked down and not responding.' This issue is largely due to the use of tokens for remote login. MoJ is in the process of moving away from using tokens to using an app for remote login. In addition, Just Store should work well on or off site, thus addressing this issue for those to whom it is being rolled out.

Information on shared drives is not easily discoverable from a corporate point of view (although staff we interviewed found it easier to find their own or team information on shared drives than in TRIM). There is a large amount of information held on the shared drives and it is not possible to search across them all. MoJ is currently considering what approach to take with the shared drives as it moves to Microsoft Office 365. As part of this work it needs to consider how to make information that is held there more discoverable. See **recommendation 4**.

Emails held within PSTs or personal mailboxes are not accessible to anyone other than the individual who created them. MoJ already has a clear policy in place stating that personal drives are not to be used for corporate information and that emails of corporate value need to be saved to TRIM or shared drives (in the future Just Store). KIM Champions and Information Managers should encourage and check that staff are following this policy. It will also be easier to move emails to Just Store which should encourage staff not to just leave them in their inbox. **See recommendation 4**.

It is possible to control access to folders within TRIM. Information Managers manage access permissions in their business areas. The KIM team recommend that they use work groups rather than named users: setting permissions by named individuals raises a risk that the information will become inaccessible once those individuals leave the organisation. Information Managers have to ask the KIM team to add new individuals to permission groups. Access permissions in Just Store operate in

virtually the same way as in TRIM. The KIM team intends to give Information Managers privileges to add members to the work groups, which should make permissions easier to manage.

In order to apply access controls to shared drives, a request needs to be made to IT. This process is cumbersome and there is a risk that sensitive information is accessible to the wrong people. In addition, access permissions are not always removed or changed when people leave the team. As MoJ forms a plan for the shared drives, it needs to consider how it will better and more effectively control access to the information held there. **See recommendation 4.**

TRIM has good search functionality. There are several ways of searching including browsing the file plan, searching using record number, and building an advanced search using different fields. However, staff are not always aware or confident in using this, preferring to use simple keyword searches that are much less effective. Staff we interviewed spoke about the search being slow, not getting the right search results and, in some cases, not being able to find documents that they themselves had filed into TRIM. It is anticipated that searching Just Store will be easier and more effective. The planned training programme to accompany the Just Store roll-out should help to ensure that staff understand how to use the search function. There are also early thoughts around creating some specialist training on search. Information Managers also play an important role in supporting staff in getting the best out of search.

## 2.2 The continuity of digital information

Goal: The organisation is taking proactive steps to ensure the continuity of its information, over time and through change.

### Oversight of information

MoJ has good oversight of what information is on TRIM but does not have a detailed understanding of the information on the shared drives. At present, there is no clear idea of volumes (it is estimated that there is around 15+ years [57TB] worth of documents and datasets) or what is on them, although there is a recognition that they are likely to contain information of value both from a business and historical perspective. MoJ needs to develop a plan to deal with the information on the shared drives (see also section 2.1), including identifying material of business and/or historical value and migrating this elsewhere, or deleting or transferring to The National Archives. There are plans to acquire DROID (The National Archives' file profiling tool) and this will help MoJ to get an overall sense of what is on the shared drives and help to identify duplicates. **See recommendation 4.**

There is around 2TB of information on TRIM and a proportion of this will be migrated to Just Store. The KIM team has already been encouraging business areas to carry out some housekeeping around their records prior to the move to Just Store. MoJ already has experience of exporting from TRIM due to a number of machinery of government changes. MoJ has already identified and clearly marked around 5,000 folders that are of historical value and will in due course be transferred to The National Archives (see section 4.1).

MoJ has factored in digital continuity considerations to its information asset governance framework. For example, the Information Asset Register (IAR) template includes a prompt for Information Asset Owners (IAO) to manage digital continuity risks and digital continuity is covered in IAO guidance and workshops. **This is good practice.**

### **Digital continuity planning/IT change**

Relationship between KIM, the Records Management Service (RMS) and IT is improving. The KIM team is linking up with Digital Technology on the KIM strategy and Just Store project. In terms of IT procurement, during the acceptance-into-service stage, the DRO and the Head of Data Access and Compliance Unit (DACU) are asked to confirm that records management and data protection requirements are

met. However, Digital Technology may not necessarily fully understand the need for information and records management functionality; for example, there was a suggestion that staff could just save their information on One Drive. Continued communication and collaboration between KIM, RMS and Digital Technology should help to mitigate this, particularly around future plans for the shared drives. **See recommendation 4.**

Digital continuity is being embedded into existing processes where possible. Risks around legacy systems and digital continuity are recognised as part of the MoJ risk management process. The requirement to consider digital continuity risk is included in the Department's IAO role description and the IAR template includes the requirement to record whether a digital continuity risk assessment has been completed. **This is good practice.**

## 3 Information risk, governance and oversight

### 3.1 Recognising information risks

Goal: The organisation defines and manages information risks to minimise threats and maximise opportunities.

#### Documenting and defining information risks

The Ministry of Justice (MoJ) has made good progress in ensuring that information risks are recognised and managed corporately. The Information Risk Policy defines information risks as threats to:

**CONFIDENTIALITY-** Resulting in unauthorised access or disclosure of information

**INTEGRITY-** Resulting in inaccurate, incomplete or corrupted information

**AVAILABILITY-** Resulting in authorised users being unable to access information when required.

The Senior Information Risk Owner (SIRO) Board Risk Register for February 2016 lists risks around cloud services and third-party supplier compliance, but it is positive to also see risks listed on digital continuity and legacy systems:

**RISK:** Unknown vulnerabilities in legacy systems.

**CAUSE:** Systems no longer supported and/or not patched up to date.  
Documentation out of date.

**EFFECT:** Confidentiality of systems and information may be compromised.  
Information on systems may not be accessible when required. Information including metadata may become corrupted.

And information management:

**RISK:** Information (electronic and paper) and records are not stored in correct locations and/or retained for correct lengths of time.

**CAUSE:** Insufficient understanding by the Department of the value of good information management. Lack of an overall information management strategy. Managers and staff not fully aware of the need to correctly organise, make available and destroy/archive information. Current technology provision makes it difficult for staff to manage information well.

**EFFECT:** Department cannot implement the governance to support the information principles. Reputational damage to the Department. Harm and/or distress to individuals, breach of information legislation. Adverse impact on compliance with Goddard Inquiry. Increased probability a technical compromise of systems will lead to a data breach.

Appropriate mitigating actions are listed covering policy, guidance, training, disposal, and analysis of shared drives. MoJ should include among these mitigating actions the role of SIROs, Information Asset Owners (IAOs), and Knowledge Champions in driving a supportive culture promoting policy and compliance. MoJ should also include risks around cyber security and reflect the impact of IT change here or elsewhere within in its risk framework. **See recommendation 3.**

Understanding of information risk across MoJ is improving. However, some of the staff we interviewed still saw this as being about protecting personal data and physical security rather than information availability. In addition, the SIRO noted that the availability aspect of information risk was not on his radar yet, and would be commissioning the Head of Information Operations Division and Digital Technology to address this. Such factors should be brought out in the existing definition. Ongoing training, guidance and communications will continue to embed understanding of information risk. **See recommendation 3.**



## Implementing an information risk management approach

There is a good framework in place for managing risk within MoJ. The risk of the loss or inappropriate disclosure of information is managed as part of business risk and by a network of Senior Information Risk Owners (SIROs) across MoJ. The Departmental SIRO chairs the MoJ SIRO Board, whose role is to ensure that MoJ achieves the required standards of information assurance and compliance. The SIRO Board reviews the MoJ Information Risk Register that covers significant information risks from across the Department.

There is a strategic risk register that includes 'top down' broad strategic risks and 'bottom up' business risks. According to the Risk Management Policy:

'The appropriate board or senior management team for each business area will regularly review their risk register. This should include scrutiny of the effectiveness of controls in reducing the level of unacceptably high risks. Any higher scoring risk that does not reduce in line with its projected target score and date must be subject to strong challenge and/or escalation. The appropriate senior manager should formally sign off their register to verify accuracy and transparency and to show that they accept responsibility for delivering the mitigating actions.'

Programmes must also agree a documented Risk Management Strategy that must lay out the escalation route for risks and the threshold above which a risk will be escalated. The escalation route should lead to the business area that initiated the programme, which will permit further escalation to MoJ strategic level if required.

The SIRO Board and Information Assurance Leads (IA Lead) Committee play a key role in the risk management process. The purpose of the SIRO Board is to ensure that MoJ 'achieves the required standards of information assurance and compliance' through agreeing strategies and policies, supporting and prioritising information risk management activities, and ensuring that there are adequate and joined-up governance structures. Through this board information risks are visible to the SIRO, and group SIROs who are senior business representatives. **This is good practice.**

We gained a good level of assurance that the above risks were subject to active scrutiny from the SIRO board and its members.

The IA Leads Committee supports the MoJ SIRO Board in ensuring that MoJ complies with HM Governments' information assurance policy and manages information risk robustly. Its purpose is:

- To agree priorities for escalation to the MoJ SIRO Board and make recommendations on action.
- To oversee progress on the mitigations of risks on the corporate information risk register and agree escalation of emerging risks.
- To keep processes for assessing compliance with information assurance policies under review, and ensure robust monitoring regimes are established across the department.
- To support the SIRO Board in its work to establish a culture of good information handling in the department and oversee the delivery of communications and training for staff.
- To share best practice in information assurance management and take a more joined up 'departmental' approach to day-to-day IA issues.

Executive Committee get to see all risks on the SIRO risk register annually as these are included in both the Cabinet Office Report (Departmental Security Health Check) and the Annual Report on Security and Information Risk Management which the SIRO and Departmental Security Office provide to the Permanent Secretary. There is a process for escalation of information risks when required.

MoJ has been very engaged with The National Archives' work on information assurance and risk. MoJ had a Board briefing on information assurance and risk from The National Archives in 2014. However, there are a number of new senior staff and a revisit would be a useful way of ensuring continued engagement and awareness here. MoJ should therefore liaise with The National Archives on organising a Board briefing for the current Board. **See recommendation 3.**

KIM was subject to an internal audit in 2013. A follow-up report in 2015 showed there was still some outstanding work around the KIM Strategy (for instance, it needed to be formally agreed and aligned with Central Information Assurance Branch [CIAB] work) and testing of records in business areas by IMs (some local testing was in place but not yet formalised and the IM role was under review).

## 3.2 Establishing control

Goal: The organisation has effective governance structures in place that foster communication and strategic planning.

### **Governance structures**

MoJ has a SIRO Board (see section 3.1 above) which includes members from IT, Information Assurance and KIM including the DRO as well as representatives from across the business. This provides an opportunity for joint planning and communication. In addition, IA, Records Management (RM) and Knowledge and Information Management (KIM) colleagues are based in the same business area, and we saw evidence that they work closely together. In addition, the relationship between KIM, RM and IT has improved since the last IMA.

### **Supporting the business**

The KIM team currently consists of six staff: a Head of KIM, a Head of Electronic Records Management (ERM), a Senior KIM Advisor, two Electronic Document and Records Management (EDRM) System Administrators and a KIM Advisor. The KIM team provides training, guidance and support to the business, leading on Knowledge Management within MoJ, with responsibility for the Just Store project and overseeing the KIM Champion and Information Manager networks. The KIM business plan for 2015-16 states that the KIM team should:

1. Enable MoJ staff to manage their electronic information effectively, in order to help MoJ operate more efficiently and flexibly; mitigate risks and maintain and preserve the corporate record
2. Safeguard MoJ's electronic information through provision and maintenance of a new, fit-for-purpose EDRM
3. Embed a culture of good information-handling and knowledge management in the culture of the organisation
4. Run our business effectively and efficiently

MoJ needs to ensure that, as the KIM and Digital Strategies take shape, the business plan for 2016-17 is fully aligned with these. **See recommendation 1.**

The KIM team, with the Records Management Service (RMS), provides a good service to the business. Staff interviewed generally felt they could get the advice and support they needed in a timely fashion. The KIM team is also actively joining up with other areas of work across MoJ. For example, the Senior KIM Advisor is a member of the KIM Policy Profession Working Group supporting them in their work to improve knowledge management and encourage/share best practice.

### **Support networks**

MoJ has an established network of Information Managers (IMs). According to the role description for IMs, 'Each team has an IM and your IM is your first point of contact if you need advice or support with managing electronic information'. Their responsibilities are clearly defined and are to ensure that digital records are structured and managed appropriately in their business areas and provide support to colleagues in managing digital records. Skills required for the role include good IT skills and a willingness to learn, a good knowledge of business functions in their area, and the ability to communicate, influence and advise on records and information management. **This is good practice.** Information Managers do not have a formal monitoring role, though at least one interviewee did try to spot-check what records colleagues were saving in TRIM. MoJ should look at how IMs can play a role in any compliance monitoring process that is developed. **See recommendation 5.**

Information Managers we spoke to were keen and proactive and took their role seriously. The IM role is appointed at a relatively junior level: at least one IM felt that they were not always able to influence senior colleagues and they should be able to draw on the support of the Knowledge Champion in these situations. It was not clear whether all IMs had responsibilities in their performance objectives. Line managers should ensure that this happens and that the work that IMs do is formally recognised. **See recommendation 4.**

The KIM team oversees the IMs, providing training and guidance as required. There is an IM forum that meets quarterly and which provides an opportunity to communicate important messages, as well as discuss issues and share best practice. According to the KIM team, turnout is usually quite good. The KIM team also sends out a monthly IM newsletter via email. Most IMs felt they had sufficient time to do the role, although there was an awareness that more time will need to be given to the role during the Just Store roll-out. IMs will play a crucial role in the Just Store roll-out and MoJ should check that IMs have the right skills to support staff in this. **See recommendation 4.**

The KIM team has recently reviewed and revitalised the Knowledge Champions' network in line with the roll-out to Just Store. Responsibilities are around promoting the importance of information and records management. The role is meant to be at Senior Civil Service (SCS) level – usually Deputy Directors, although the interviews revealed at least one or two areas where this had been delegated to Grade 7 or below. Not everyone knew their Knowledge Champion or what the role entailed. MoJ should discourage delegation of the role to lower grades, although of course it is perfectly acceptable for more junior staff to help and support their Knowledge Champion. MoJ should also remind staff who their Knowledge Champion is and what the responsibilities of the role are, perhaps via the intranet. As with the Information Manager role, it was unclear whether this role was incorporated into performance objectives and MoJ should ensure this work is formally recognised. **See recommendation 2.**

### 3.3 Providing direction

Goal: The organisation gives staff the instruction they need to manage, protect and exploit information effectively.

#### Knowledge and Information management policy and guidance

MoJ's Information Management Policy was updated in March 2016. At just over just over three pages in length, it is succinct and easy to read. It clearly sets out the benefits of complying with the policy, roles and responsibilities, where to save information and legal responsibilities. As one interviewee put it, 'No-one has an excuse not to know that things should go on to TRIM.' Another stated: 'Documents you create need to go on TRIM, particularly final documents and submissions – I use it as much as possible, but I'm looking forward to Just Store.' The policy also refers to other related pieces of guidance such as the What to Keep Policy and the Records Management Services Handbook. The policy would benefit from including more about the specific responsibilities of various groups of staff, including those in information-related roles such as KIM Champions and Information Managers. The Northern Ireland Office's and Houses of Parliament's Information Management Policies are good examples of where this has been done well. The policy will also need updating as Just Store and Microsoft Office 365 are rolled out to staff. **See recommendation 4.**

MoJ has produced a comprehensive set of guidance covering all aspects of information and records management that is clear and succinct. It is clearly visible on the intranet and there are key KIM messages on the front page. Of particular note are the What to keep Policy (see below), Email Management and Vault Archiving Policy. Training and guidance is about to be updated to reflect the move to Just Store.

MoJ has continued to improve its approach to knowledge management since the last IMA and has recently updated its process and guidance for this. The knowledge

management page on the intranet has been rewritten and new guidance around knowledge capture and handover, including a head start form and guidance and a leavers checklist, has been produced. This was about to be signposted as part of the Knowledge Management campaign that MoJ has been running. MoJ has also developed 'An Audience with' sessions for senior people or for specialists in their field, in order to capture knowledge before they leave and give colleagues a chance to ask questions. Sessions were held last year when around 80 technology staff moved on. **This is good practice.** There needs to be an increased focus on knowledge transfer in the coming months, as MoJ is due to lose a number of staff as part of the Voluntary Exit Scheme. A further communications campaign in conjunction with Human Resources is planned. **See recommendation 2.**

Also of note is the information security campaign that MoJ ran from December 2015 to March 2016, which aimed to increase staff awareness and understanding of their responsibilities when handling information. The top line of the campaign was:

'It's in your hands to keep information safe, sound and shared.'

Activities included drop-in sessions, articles, emails and poster campaigns. Each month had its own theme and issues such as safe remote working, cyber security and good information handling were covered. The impact of the campaign was tested through surveys, test phishing emails, statistics on who attended events or read intranet articles and the number of people who completed the 'Responsible for Information' e-learning. Staff we interviewed generally recognised the importance of protecting and handling information appropriately, and had completed the e-learning, while several mentioned aspects of this campaign. **This is good practice.**

## What to Keep

MoJ has developed a high level What to Keep Policy and each business area has a retention schedule. There are over 95 record retention and disposition schedules that govern the departmental records. These cover all types of records and state when they can either be destroyed or kept for review after 20 years. MoJ has published these in line with Sir Alex Allan's recommendation in his Report on Records Review.

MoJ also has an Information Review and Disposal Policy that links in with the above. The what-to-keep guidance is clear, succinct and easy to read. The retention schedules are developed and updated in conjunction with business areas to ensure that these work in practice and the right information is kept to enable business areas to carry out their work. **This is good practice.**

Some, but not all, staff we interviewed were aware of the what-to-keep guidance, although the majority of interviewees seem to be making sensible decisions about what to keep, even if they were not always keeping them in TRIM. The move to Just Store provides a useful opportunity for MoJ to remind staff about this. **See recommendation 4.**

## Providing training

MoJ provides bespoke training on information and records management to business areas and this compliments the guidance on the intranet (see above). It also provides training on information assurance and risk to IAOs and other related roles and has worked closely with The National Archives on this. All staff are expected to complete the 'Responsible for Information' e-learning module on Civil Service Learning on appointment and complete refresher training each year.

MoJ recognises the importance of training when implementing a new system and a full training programme will accompany the roll-out of Just Store. There will be a two-and-a-half hour training course for Information Managers, as they will play a key role



in supporting staff on this. For end users there will be a 45-minute e-learning session on Just Store with a test at the end to cement learning. MoJ has been looking at the e-learning that Home Office used for their 'imanager' roll-out. The training will cover not only how to use the system, but also why it is important and what the benefits of using Just Store are. Ideally the end user training should be mandatory, although no firm decision had been made on this at the time of the assessment. There will also be floor walkers on hand to provide support as well as support from the Information Managers. The IM Just Store training will continue to run as necessary and there are also early thoughts about putting together specialist searching training for Just Store.

### 3.4 Measuring impact

Goal: The organisation measures performance in practice and takes informed risk-based action as a result.

#### Measuring compliance with policy

As of yet, there is no formal process for measuring compliance with information and records management policy and guidance in the business. MoJ did do a series of health checks around two years ago using the Information Managers, and an internal audit recommended that these continue. However, it has not been possible to continue the programme due to resourcing issues. MoJ would benefit from developing a monitoring process and should explore the work that HM Treasury and Home Office have done here. MoJ should also state how it intends to monitor compliance in its Information Management Policy. **See recommendation 5.**

#### Assessing progress against strategic goals

As covered in section 1, MoJ is currently drafting its KIM strategy. Once the strategy has been written and signed off, MoJ needs to ensure that it has a process for reporting on progress to the senior team, via the SIRO Board, and that there is an opportunity for them to challenge and interrogate progress. **See recommendation 1.**

## 4 Records, review and transfer

### 4.1 Oversight of records and selection

Goal: The organisation understands the value of its records and can consistently identify those with enduring historical value.

#### Position of the Departmental Records Officer (DRO)

The DRO/Head of Records Management Service (RMS) sits within the Information Operations team along with the Head of Knowledge and Information Management (KIM). Under the DRO sits a review team of 11, including one head, six staff dealing with Court records and four staff dealing with MoJ records. There is also a team of 12 that make up the Branston-based Registry team and a team of seven that deal with records scheduling and archives. The DRO and her team are fulfilling all aspects of the role as detailed in The National Archives' guidance. The Records Management Service works very closely with the KIM team, and the DRO and the Head of KIM have a good working relationship. The DRO also sits on the Senior Information Risk Owner (SIRO) Board and has a direct line to the SIRO via the Head of Information Operations. **This is good practice.**

Current priorities for the team are, according to the draft business plan for 2016-17:

- Improve the integrity and availability of records held in both on site and off site storage and ensure the reliability of records.
- Work within the legislative framework (i.e. Public Records Acts; Data Protection Act 1988; Freedom of Information Act 2000) and in accordance with guidelines set by independent inquiries to obtain, store, safeguard and preserve records, making them available to the public where appropriate. All records are reviewed, preserved or destroyed at the appropriate time and in an appropriate manner.
- Ensure all necessary Records Management action is taken in the event of prison/office closures, machinery of government changes.

- Ensure e-review process is carried out, working with The National Archives and eDRM to commence facilitation of sensitivity review.
- Identify cost savings on storage costs,

### **Oversight, control and use of records**

MoJ has good oversight of MoJ HQ paper records. Paper records are stored off site at TNT and at the Branston Registry. There is also registry space at Petty France where files can be stored while they are being reviewed. MoJ has so far been able to provide accurate figures for the bi-annual RecordsTransfer Report.

Staff we spoke to were able to access the digital and paper records they needed, although there were some issues about searching for digital records (see section 2). It was unclear how far staff were using records outside their own business areas and MoJ could do more to encourage this, possible through its work on knowledge management. The move to Just Store should also facilitate greater information sharing. **See recommendation 4.**

The National Archives' Government and Remote Services team, which oversees requisition of files from The National Archives, has a good working relationship with the Records Management Services team at MoJ. There were no significant issues in terms of business-as-usual requisitions, outstanding or misplaced records.

### **Appraisal and selection**

MoJ uses Operational Selection Policy (OSP) 40 to inform the appraisal and selection of crown court records. The OSP has recently been updated and will be updated further in the future. For other records, MoJ has used The National Archives' general selection criteria to create some selection guidance that relates to MoJ specifically. Staff review about 40 files each day and quality checking is carried out by the review manager: for new staff 100% checks are carried out. All records reviewed also go through a check to see whether they might be of relevance to the Independent Inquiry into Child Sexual Abuse (IICSA): records that may be relevant

are then kept in a separate, secure area. MoJ's appraisal work is of a high quality and The National Archives' Information Management Consultant (IMC) is usually able to approve MoJ selection decisions without the need for re-review.

At present, MoJ still does file by file review for paper records and does not use Series Level Appraisal Questionnaires (SLAQs). Up to now, it has been hard to adopt a more macro approach as little series level information is available and file topics tend to be quite random. However, the volume of paper files doubles between 1992 and 1996, so MoJ will need to start looking for ways to speed up the paper appraisal process through using macro methods where possible. **See recommendation 6.**

MoJ has developed a process for appraisal and selection of digital records on TRIM. Work on this began around two years ago. File by file review was tested, but proved to be too labour-intensive for digital records, so MoJ is taking a macro approach to reviewing at level 3 in TRIM. According to the review team, file titling in TRIM is quite good but what staff actually file in containers can vary, so checks are required. Reviewers have a target of reviewing around 100 files a day. As experience of reviewing digital records grows, reviewers are noting patterns – such as areas where they have not selected anything for the last two years – that will aid selection in the future. Once records have been identified for selection, the file path is exported from TRIM onto a spreadsheet and review comments are added. The National Archives' IMC has access to a TRIM account and can access the spreadsheet to make comments/sign off decisions. MoJ has reviewed records in TRIM up to 2014 and around 5,000 folders have been identified and marked for transfer to The National Archives. These records will be migrated to Just Store along with the rest of the records in TRIM and will be transferred to The National Archives in due course from there (they are not due for transfer until 2022). There will be a records center for each year of selected material transferred to Just Store. The same approach to appraisal and selection will be applied to new records created in Just Store. **This is good practice.**

MoJ has not yet appraised and selected material on the shared drives, though it recognises that there will certainly be records of historical value held there. MoJ needs to determine how it will appraise and select information on the shared drives and develop a process for this. Analytical tools such as DROID (The National Archives' file profiling tool) and e-discovery tools would help this process and The National Archives can provide more advice on this. **See recommendation 6.**

## 4.2 Implementing disposal decisions

Goal: The organisation understands the process for records disposal and consistently implements decisions in line with defined plans.

### Triggers for disposal

Processes are in place to ensure that disposal of paper files is carried out in line with MoJ's agreed retention and disposition schedules (see section 3.3) and there is an annual destruction exercise each January. This work is carried out by the RMS team, including staff at the Branston Registry and at TNT. Disposal is largely on hold at the moment due to the requirements of the Independent Inquiry into Child Sexual Abuse (IICSA), which is causing difficulties in terms of storage costs and space. TNT staff have been trained to seek out files that are unlikely to have relevance to IICSA. These files are then checked, listed, and the Branston Registry team signs off destruction. One member of the RMS team has been assigned the role of single point of contact for the IICSA.

MoJ has applied retention periods to TRIM and a process is in place for enacting these. Retention and disposal instructions will be transferred to Just Store when information from TRIM is migrated.

MoJ has not yet applied disposal to the shared drives and this should be part of any plan relating to the shared drives (see sections 2.1 and 2.2). **See recommendation 6.**

## **Sensitivity review**

The review team carries out sensitivity review of paper files. FOI exemptions used are mainly Section 40 and Section 38 in relation to sensitive personal information. Closure is rarely applied to policy material. Occasionally reviewers will consult with the FOI team or with The National Archives if there is something they are not sure about. The team will also consult with other government departments about sensitivity as required. As with appraisal and selection work, sensitivity review decisions are quality checked before being passed to The National Archives for approval. One member of the review reported that it was in their performance agreement to achieve a certain level of accuracy. From The National Archives' perspective, no major issues were reported around sensitivity review/applications to the Advisory Council.

MoJ has trialled manual sensitivity review for digital information as part of the Digital Transfer project. Although they managed to review more than expected, this is not possible at scale: MoJ should consider using data analytics and other tools to assist the process of sensitivity review and to carry out redaction. They have visited Home Office to look at the work they are doing with e-discovery software; however, cost is likely to be a significant barrier. MoJ should continue to follow the work that The National Archives and other departments are doing, and should consider the possibility of joining up with other departments to share a solution. **See recommendation 6.**

## **Transfer and planning**

At the beginning of each year, the review team go through file listings to see how many records are due for review that year. The review manager then plans which resources are required where. Records are called back in batches of just under 500 from TNT and then sorted into file number order in the MoJ registry at Petty France. Once records have been selected for transfer, MoJ produces a Series Level Time Plan (SLTP) that gives the team a timetable for the transfer process. According to

Record Transfer Report figures, MoJ is progressing well with review and transfer and is slightly ahead. There are some delays around the Judicial Committee of the Privy Council legacy records but these should be transferred in 2016.

There have been a few issues regarding cataloguing and preparation work not being quite up to the required standard. The Review Manager is addressing this by encouraging the team to quality-check work before it is sent and by signing the team up for The National Archives' new e-learning module on preparation of records for transfer.

At present, the review team is able to keep up with the transition to the 20-year rule. However, the volume of paper files increases in the 1990s and MoJ is aware that it will need to explore methods of speeding up the process of appraisal and selection of paper files (see section 4.1). **See recommendation 6.**

The RMS and KIM teams are fully engaged with The National Archives, in particular with their Information Management Consultant. MoJ is involved with the Digital Transfer Project as a pilot department and has regularly attended. Staff from MoJ attend the quarterly Information Management Liaison Group sessions and members of the team have spoken at this event in the past. Team members have also attended The National Archives' training courses on appraisal, digital continuity, cataloguing, preparation and digital transfer.