

# **Information Management Assessment**

**Her Majesty's Revenue and Customs**

**January 2011**

<b><u>PART ONE: EXECUTIVE SUMMARY</u></b>	<b><u>2</u></b>
<b><u>PART TWO: INTRODUCTION</u></b>	<b><u>6</u></b>
<b><u>PART THREE: HIGHLIGHTS AND AREAS FOR IMPROVEMENT</u></b>	<b><u>8</u></b>
<b><u>APPENDIX ONE: SUMMARY OF RECOMMENDED ACTIONS</u></b>	<b><u>28</u></b>
<b><u>APPENDIX TWO: IMA COMMITMENT</u></b>	<b><u>32</u></b>
<b><u>APPENDIX THREE: GLOSSARY</u></b>	<b><u>33</u></b>

Date: January 2011

© Crown copyright 2011

## PART ONE: EXECUTIVE SUMMARY

HMRC should be proud of its achievements in raising levels of understanding, awareness and compliance in relation to information security and assurance. The Executive Committee has provided high-level support, visibility and direction for data handling with a solid governance structure that reinforces the importance of securing personal information. Preventative measures are in place and all the personnel interviewed as part of this Information Management Assessment (IMA) were found to be aware of their responsibilities. The potential benefits of good information management are, however, far less appreciated. HMRC now needs to build on the progress made and embed the principles that underpin good information management.

HMRC is a large and complex organisation with many diverse and legacy IT systems. The challenge for HMRC is to make best use of its systems, its information and ensure consistency across the organisation. Our IMA is intended to provide a focus for the department in addressing these challenges. Even in a difficult financial climate, we are of the view that HMRC should continue to invest in developing good information management. This work should be underpinned by ensuring existing governance covers both information security and information management.

The IMA highlighted the fact that some areas of the business were not fully engaged with knowledge and information management (KIM), did not understand why KIM matters nor how information management supports daily activity. HMRC needs to continue to encourage an information management culture within the constraints of a tight information assurance environment. The support of staff at middle-management level is essential to reinforce cultural and behavioural changes. Many of the managers the audit team met were focussed on meeting their business or directorate objectives, without strategic consideration of how good KIM practices could help to deliver corporate objectives. HMRC needs to consider how it should engage those managers. Consideration should also be given to the further development of support networks where issues can be examined, corporate solutions agreed and good practice shared.

Risk management of information security and assurance is at a high level, and rightly remains a top priority. Commendably, KIM is also part of the KAI

Directorate's risk register. However, we recommend that KIM risks are held corporately and that the potential impact of poor information management is communicated across the whole organisation.

HMRC operates in an increasingly information rich environment and creates, uses and interrogates vast amounts of information. It needs to be confident that it is capturing and sharing the information appropriately and can locate information if required to do so. HMRC should continue its work to improve its understanding of the complex information landscape it works in so that it can be confident in finding, keeping and sharing its business information efficiently.

HMRC has a number of specialist roles with responsibility for information security and assurance and knowledge and information management. This visible investment is to be commended. However, we saw a lack of understanding among staff about how these roles fit together and also about their specific objectives and responsibilities.

HMRC has taken steps to bring structure to its "desktop" information by developing a series of Controlled Access Folders (CAFs) to store business information that is not held in head of duty systems and databases. All directorates are migrating to CAFs by end of March 2011. HMRC needs to ensure that corporate standards are adhered to and maintain a degree of consistency of approach, for example in the correct application of folder- / file-naming conventions.






HMRC still has a wealth of paper records, a situation that is unlikely to change in the near future. There were differing approaches to the management of paper files across the department and HMRC needs to consider a more systematic approach to managing paper records, particularly their disposal. We found instances where locally implemented retention policies differed from those published on the corporate website.

HMRC has made a good start in its information management journey by embedding good information assurance and security practices. If HMRC addresses the recommendations outlined in this report The National Archives is confident that it will be in a good position to achieve its core KIM objectives.






## Risk Matrix

The Risk Matrix result is a culmination of the pre-assessment analysis, onsite interviews and evidence submitted.

### Governance and Leadership

Strategic management		Good
Business objectives		Good
Management controls		Development Needed
Resourcing		Good
Risk management		Good


### Records Management

Creation		Satisfactory
Storage		Development Needed
Appraisal, disposal and transfer		Development Needed
Sustainability of digital records		Development Needed
Management		Satisfactory

### Access to Information

FOI/Data Protection		Satisfactory
Re-use		Satisfactory
Security		Best Practice






### Compliance

Staff responsibilities and delegations		Satisfactory
--	---	--------------

Policies and guidance		Good
Training		Satisfactory
Change management		Satisfactory

**Culture**

Commitment		Good
Staff understanding		Satisfactory
Knowledge Management		Satisfactory

<b>Key to Colour Coding</b>	
	<b>Best Practice</b>
	<b>Good</b>
	<b>Satisfactory</b>
	<b>Development Needed</b>
	<b>Priority Attention Area</b>

## PART TWO: BACKGROUND

### **Information Management Assessments**

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

<http://www.nationalarchives.gov.uk/information-management/our-services/ima.htm>

### **The Business of Her Majesty's Revenue and Customs (HMRC)**

Her Majesty's Revenue and Customs (HMRC) came into being on 18 April 2005, as a result of the merger of Inland Revenue and HM Customs and Excise Departments. HMRC's headcount as of October 2010 is 74483, which equates to 67226.31 full time employees nationally and internationally in over 450 sites.

[http:// www.hmrc.gov.uk/index.htm](http://www.hmrc.gov.uk/index.htm)

### **Knowledge and Information Management (KIM) in HMRC**

KIM in HMRC is part of the remit of the Knowledge, Analysis and Information (KAI) Directorate. KIM activity is carried out across HMRC within the different Lines of Business. KAI is working with senior managers and other stakeholders to establish information and knowledge management as key building blocks for delivery of HMRC strategy.

KAI has the role of providing the lead in these activities, with responsibility for KIM strategies, policies, guidance and toolkits. Working with business areas, KAI helps them implement the strategies and policies and runs a range of projects to meet specific business requirements within an overall strategic framework.

## **Methodology**

The IMA took place between 15 March and 22 April 2010, the Assessment Team undertaking 90 interviews and visiting 6 sites. The team comprised:

- Standards and Assessment Manager
- Head of Standards
- Information Management Consultants
- Standards Adviser
- Digital Continuity Project Manager
- The Cabinet Office's Head of Information Security and Assurance

## **Assistance provided by the department**

The Assessment Team are grateful for the co-operation and assistance of all staff within HMRC and especially that of staff within KAI in facilitating the on-site assessment.

## PART THREE: HIGHLIGHTS AND AREAS FOR IMPROVEMENT

### **Governance and Leadership**

#### **Strategic Management**

The Executive Committee of Her Majesty's Revenue and Customs (HMRC) has provided high-level support, visibility and direction for information security and assurance across HMRC. HMRC senior management is open about the effect of the 2007 data losses and the Data Handling Review in raising the profile of the information security and assurance agenda. These had a significant impact, driving the setting of internal standards and reinforcing secure working practices. The Senior Information Risk Owner (SIRO) in HMRC is the Permanent Secretary for Tax and is a member of the Executive Committee. This endows the role with a level of importance, responsibility and visibility that is to be commended and represents best practice.

HMRC has developed and implemented a solid governance structure that reinforces the importance of securing personal information; this was evident across all levels of HMRC. However, despite the effectiveness of information security and assurance for its core structured data, the department does not consistently apply effective information management assurance procedures to its wider information and records of a non-personal nature. There was evidence of good local practices, but these were neither centrally coordinated nor consistently applied.

KAI, with support from the Executive Committee, worked hard to raise the profile of KIM in the lead up to the IMA. This momentum needs to be maintained.

**Recommendation 1: HMRC should continue to invest in the structures that have allowed for significant progress on information assurance, and, more recently, management of information, particularly during this period of efficiency savings.**

## **Management Controls**

HMRC has gained Executive agreement for its KIM strategy. The strategy is owned by the KAI directorate, whose Director is also the Departmental Records Officer (DRO). Now that the strategy has been agreed, HMRC needs to test existing policies, procedures and guidance to ensure they align with it. HMRC also needs to ensure that these policies are fully implemented.

**Recommendation 2: HMRC should ensure that checking of compliance with KIM policies and standards is included as part of regular internal assurance processes.**

HMRC does not currently have a coordinated approach to reporting progress on implementation of the KIM programme. KAI would be well placed to provide assurance that standards are being met.

**Recommendation 3: HMRC should develop a KIM performance measurement regime reporting to the SIRO.**

## **Resourcing**

HMRC has created a range of specialist roles with varying levels of accountabilities and responsibilities for information security, assurance and KIM. These are Data Guardians, Information Champions and Information Partners, in conjunction with recognised records management specific roles such as the Departmental Records Officer (DRO). This visible investment is to be commended. However, there was confusion expressed during the assessment about the responsibilities and overlap of these roles. Both post holders and staff members need clarity to enable HMRC to gain full benefit from the available expertise. The GKIM Professional Skills Framework could

be a useful point of reference in this exercise. 1

**Recommendation 4: HMRC should better define the various KIM roles within the business, provide adequate support for those roles and improve communication of these roles to staff.**

### **Risk Management**

Since the 2007 data losses, HMRC has worked hard to ensure that the security risk to its information is minimised. This remains a top priority in the department. For example, all managers have information security as an objective in their personal development plans and all staff are provided with a printed desk guide. However, more needs to be done to manage wider information risks including the risk of not fully exploiting the information that is available. Each business area is responsible for assessing and managing its information risks”.<sup>2</sup> While there is central assurance of security risks and corporate risk management in general there is no effective central assurance of the management of KIM risks.

**Recommendation 5: Building on progress made, HMRC should take advantage of the Information Assurance programme, and now expand the agenda to include the benefits of good information management.**

HMRC has invested heavily in protecting its information through strong controls on data handling. These controls sometimes add cost and could occasionally be perceived to have an adverse impact on the business. HMRC recognise the imperative to secure personal and sensitive data, hence the need for strict controls that can sometimes impact on timescales for release of data.

---

<sup>1</sup> <http://gkimn.nationalarchives.gov.uk/framework.htm>

<sup>2</sup> Guidance on managing information risk for government is detailed in “Managing Information Risk: A Guide for Accounting Officers, Board Members and Senior Information Risk Owners <http://www.nationalarchives.gov.uk/documents/information-risk.pdf>

**Recommendation 6: HMRC needs to encourage staff to explore how they can maximise data flows to support delivery of its objectives while maintaining high levels of data security.**

HMRC creates, controls and handles large sets of data and information, most of which is held on tax specific “heads of duty” IT systems. The department does not have a full Information Asset Register (IAR) as defined within Digital Continuity Guidance.<sup>3</sup> There is currently no corporate data model, although the organisation is currently developing its information architecture. The identification of information assets and information asset owners, through an information inventory, is in progress, although with such extensive data holdings it is recognised that this must be a staged process. The compilation of the inventory is being driven by the identification of the key processes that underpin the business.

**Recommendation 7: Whilst The National Archives acknowledges the challenge in this complex information environment, HMRC should continue working to define key processes and their related information/data flows where relevant.**

**Recommendation 8: HMRC should continue to improve its understanding of its key information assets.**

Teams know that data integrity is important to deliver HMRC services, but data integrity projects are all managed at a local level or run on an ad-hoc basis.

**Recommendation 9: HMRC should harness the good work that has been initiated by local data integrity projects, sharing lessons learned across the organisation.**

---

<sup>3</sup> Definition contained in <http://www.nationalarchives.gov.uk/documents/identify-information-assets.pdf>

## **Records Management**

### **Creation/What to Keep**

HMRC works in an increasingly information-rich environment, creating, using and interrogating vast amounts of information on a daily basis. HMRC is clear on what its top business-critical processes are. Most of the data held in HMRC is customer data which is collected in the process of conducting HMRC's statutory function and is supported by its statutory powers. Most of this information is stored on the tax specific heads of duty IT systems.

As well as customer data, HMRC also holds policy and management information. Across all areas of its information HMRC needs to be confident that it is capturing the right information, sharing the right information and is able to locate that information if required.

HMRC identifies key information within a wide range of published documents and web pages. HMRC would benefit from drawing this together into a clear policy statement that identifies their key information and the drivers for holding this material.

### **Recommendation 10: HMRC should work closely with The National Archives and adopt the "What to Keep" guidance and approach.**

HMRC has to ensure that it can continue to manage, use and access the information within its heads of duty systems. Some of these systems, in line with the compliance regime at the time, were designed to have no disposal function. HMRC needs to meet Data Protection Act (DPA) requirements and also free up storage space. Revised retention schedules for legacy systems should therefore be introduced and retention issues tackled whether automatically or manually.

### **Recommendation 11: HMRC must introduce and implement appropriate retention schedules for heads of duty systems.**

HMRC recognises that improvements to data quality are required to maximise its ability to use its information to support the business. There is widespread duplication of information, driven by fragmentation of ownership and loss of trust in the integrity of information which is shared within the business. There is a culture of “hold many” rather than “hold once”.

Information asset owners have been identified at Executive Committee level but owners need to be identified at lower levels in the organisation.

**Recommendation 12: HMRC needs to ensure that the owners of significant information assets are urgently identified at below Executive Committee level, agreed and assigned and that this is communicated appropriately.**

### **Storage**

The organisation has developed a series of Controlled Access Folders (CAFs) to store case, policy and non-transactional data outside the heads of duty systems and databases. CAFs will replace shared folders in the shared drives. HMRC is migrating all directorates’ sensitive information to CAFs by the end of March 2011. CAFs, if used to their full potential, would enable HMRC to mitigate risks identified with its shared areas. These latter are not open to anyone outside HMRC staff but access to them is often insufficiently regulated and controlled. Access to CAFs can be restricted to discrete business groups, projects or used as a collaborative tool.

Some business areas see the migration to CAFs as an opportunity to prune files and delete obsolete material, consider file structure and assign folder owners. HMRC needs to harness and disseminate good practice on CAF migration.

**Recommendation 13: HMRC should ensure business areas rationalise and delete files on migration into CAFs, sharing good local practices to facilitate the process.**

Implementation of the CAF guidance was inconsistent. Responsibility for the creation of the CAF was often delegated to individuals interested in IT, or who had another KIM or administrative role. HMRC should review how CAF Information Managers are selected.

**Recommendation 14: HMRC to ensure that appropriate people with relevant skills are selected to fulfil the CAF Information Manager roles.**

**Recommendation 15: HMRC should conduct compliance checks to ensure the integrity of the CAF creation and management process.**

## **Retention**

It is HMRC policy that individual business areas develop and apply their own retention policies and schedules based on an overarching policy and assurance framework. The Assessment Team found examples where there was inconsistent application of published retention policies. By contrast, some areas had produced “desk aids / help cards” for their staff to help with disposal decisions. This is an area of good practice that HMRC could build on. We also found that there are insufficient checks on the effectiveness of the schedules.

**Recommendation 16: HMRC to ensure that corporate guidance is followed and that all areas have approved retention and disposal schedules that are fully implemented.**

HMRC creates, uses and stores a mass of paper records. While paper records are disposed of securely there is a lack of consistency as to how the disposal of paper files is managed. The Assessment Team did note that as part of a central initiative in 2008/9, a “weeding” exercise was carried out that resulted in 45k linear metres of local records being destroyed. HMRC acknowledges that such central and similar local exercises need to be carried out more frequently and in a more coordinated fashion. A systematic approach to managing the retention and disposal of paper records is necessary.

### **Recommendation 17: HMRC to implement a systematic approach to managing paper based records.**

Digital information is growing at a vast rate and there is a risk that HMRC fails to apply retention schedules to CAFs and shared drives with appropriate rigour. Without proper control there is a risk that CAFs are in danger of falling into the same unmanaged state as some of the previous shared drives. Whilst HMRC is in the process of an IT rationalisation programme that will address some of the issues with the electronic storage of information, the sheer number of servers and the volume of storage available increase the risk of poor information management in the department.

### **Appraisal, Disposal and Transfer**

HMRC has developed Appraisal Reports for its core business records. These identify key records that need to be preserved and maintained by HMRC, including customer records to which retention periods are applied, and those that need to be eventually transferred to The National Archives. HMRC has also recently consulted The National Archives on the selection and disposal of case files and agreed what material will be selected for transfer. This is in accordance with The National Archives Acquisition and Disposition Strategy and Operational Selection Policies.

HMRC has transferred 3 metres of material to The National Archives over the last three years. In the last year, however, HMRC has proactively identified and disposed of a great deal of paper records, and has identified a significant amount of material for transfer. It is important that resources continue to be allocated for this work to ensure that HMRC's key information is preserved.

### **Sustainability of Digital Records**

In common with all other government organisations, HMRC needs to take active steps to ensure its key information assets remain available and usable

as needed over time.

HMRC has a number of compelling business drivers to ensure the long-term continuity of its information assets. These include the fact that it holds sensitive information about individuals and organisations, with records sometimes spanning decades. The nature of its business and its contact with the majority of citizens means HMRC is also exposed to public scrutiny. HMRC's ability to find and act on authentic information at the right time is critical to its reputation.

HMRC has no formal process for managing digital continuity through technological change. HMRC is revising its approach to technology change projects, to move towards a process in which the lines of business specify outcomes and the IT function determines how to deliver these. This approach should have a positive impact on the organisation's ability to manage digital continuity during technological change.

HMRC faces a number of challenges in sustaining its records. Its data holdings are exceptionally large, even within the context of central government. HMRC is also heavily reliant on bespoke and legacy IT systems. HMRC has made progress towards ensuring it can sustain the continuity of its digital information. In particular, it has strong leadership from the SIRO and CIO combined with a strong culture of information security, which has been effectively built throughout the organisation.

**Recommendation 18: HMRC should incorporate digital continuity into HMRC's Gateway process for managing ongoing change.**

**Recommendation 19: HMRC needs to engage with its supplier to clarify the contractual responsibilities for digital continuity and agree ongoing support in managing and maintaining digital continuity.**

**Recommendation 20: HMRC should undertake a full impact assessment prior to any technological change that may affect the completeness, availability and usability of the department's information assets.**

## **Business Developed Applications (BDAPs)**

HMRC's core business depends on a large number of bespoke and legacy software applications, which presents risks to digital continuity. For example, locally developed applications (BDAPs) are not always well documented and some have no formal support arrangements. Some of these applications may contain personal information and as such need to be managed effectively. Those unsupported by IMS are currently managed and maintained on a best-endeavours basis by the staff members who use them. The department risks loss of access to the data. Furthermore, BDAP data resides on shared drives and its dependencies are not always centrally documented or understood. The data may persist long after the application is no longer in use, presenting a risk that data which is no longer required by the business is still being kept.

HMRC recognises local application development as a risk to digital continuity and has identified funding to scope database and application rationalisation, including bringing BDAPs into the corporate infrastructure and formalising support arrangements.

**Recommendation 21: HMRC should undertake a limited review of BDAPs with respect to digital continuity in order to manage and mitigate the risks of these applications until a longer term solution has been agreed.**

## **Email**

HMRC has published guidance on the handling and storage of emails. The average size of an account is 100 megabytes, but the Assessment Team were advised that some individuals have considerably more. Staff members are encouraged to transfer important information from email into shared areas or CAFs. However, there are no checks to ensure that this happens. Emails are also not automatically deleted after a given period of time. All managers and staff should be encouraged to do regular "housekeeping" of their email accounts to ensure that information is properly stored, is not kept for longer

than it should be and is accessible.

**Recommendation 22: HMRC to carry out assurance that all staff, including managers leading by example, adhere to the email policy and do regular “housekeeping” of their accounts.**

### **Management of Information**

HMRC has a core team of dedicated KIM specialists supported throughout the organisation by a number of information assurance and information management roles. The roles are there to lead, shape and monitor good KIM practice across HMRC. HMRC needs to ensure good communication links between these roles. It is particularly important for the KIM roles to share examples of good practice and we suggest the creation of a networked professional community for KIM as a means of taking this forward.

**Recommendation 23: HMRC should develop information networks to share good practice across the organisation and build a professional community of shared interest in KIM.**

## **Access to Information**

### **Data Protection Act (DPA)**

The understanding of, and commitment to, securing customer information in HMRC is at a high level. Personal objectives, security checks and policies support this commitment. However, HMRC has to do more to promote staff understanding of the importance of securing personal data of its own employees. For example, whilst the information from external customers was clearly marked and secured, information on performance reviews did not have the appropriate restrictions consistently applied.

**Recommendation 24: HMRC should clarify its guidance on how internal personal information should be managed to increase compliance across the department.**

### **Freedom of Information (FOI)**

There is a clearly defined process for handling FOI queries through a network of Freedom of Information Access Officers. Although HMRC keeps a record of the applied exemptions, this information is not kept in a central area on the CAF and so is not available for staff to re-use and apply without reference to the central team.

### **Re-use/Data Sharing**

HMRC relies heavily on partnership working and sharing information both internally and externally. HMRC has approximately one hundred statutory Gateway Agreements. These formalise what information can be shared externally with other government departments, such as the Department for Work and Pensions (DWP), what procedures should be followed and how that information is to be used.

However, there is no follow up on usage of the information after external

transfer to ensure it is being used as originally intended. There are also no restrictions on how long the receiving department can keep that information, or when use of the information should cease. HMRC, as suppliers of the data, should be confident that information is used appropriately. Data Principle 5 of the Data Protection Act states that agencies need to agree on how shared information is managed.<sup>4</sup>

**Recommendation 25: HMRC to assess the validity of incorporating a review date in its Gateway memorandum of understanding covering use of its data.**

**Recommendation 26: HMRC to monitor whether data is being used as prescribed in the Gateway Agreements.**

HMRC can make further progress in assessing what other information it holds that can be anonymised and shared externally. The emphasis to date has been on securing information. The potential for unlocking some of the non-personal information held in data sets and making that available to the general public should be explored within available resources, by reference to the data holdings that are currently published on data.gov.uk.

Given the sensitivity of taxpayer data HMRC are considering alternative ways of making data available. At the moment they are piloting a “datalab” system that will allow accredited academic users access to anonymised data to facilitate detailed analysis of the tax paying population. It is hoped that this will go live in 2011.

**Recommendation 27: HMRC should identify what further information it can make available as part of the drive to open up public data.**

---

<sup>4</sup> [http://www.ico.gov.uk/for\\_organisations/data\\_protection\\_the\\_guide/information\\_standards/principles\\_5.spx](http://www.ico.gov.uk/for_organisations/data_protection_the_guide/information_standards/principles_5.spx)

## Security

Awareness of information security in HMRC is extremely high. Internal security procedures give the Executive Committee confidence that security procedures are working. However, security measures can add cost and are sometimes perceived to make it more difficult to share information.

While HMRC has addressed the processes relating to internal security and assurance, senior management recognises that the department remains vulnerable to human error or incompetence. Additionally, there was evidence that some contracting services, such as courier services, are not following security practices as rigorously as HMRC personnel. HMRC has established a process of third party assurance that has taken input from the Security and Commercial Directorates. This operates in accordance with Cabinet Office guidelines and industry best practice (using ISO 27000). A structured review is underway of the top 30 suppliers, with 22 reviews completed and a further 8 to be finished by the end of March 2011.

### **Recommendation 28: HMRC needs to further improve assurance of third-party contractors.**

HMRC's Data Security Handbook is distributed to all staff but the application of protective marking is inconsistent. For instance, there was evidence of over-classification of documents and communications in some cases and an absence of protective marking on sensitive information in others. HMRC needs assurance that documents and communications are appropriately marked.<sup>5</sup>

### **Recommendation 29: HMRC to reinforce the usage of the Data Security Handbook's guidance on Protective Marking to all staff.**

---

<sup>5</sup> HMG Security Policy Framework:

[http://www.cabinetoffice.gov.uk/media/207318/hmg\\_security\\_policy.pdf](http://www.cabinetoffice.gov.uk/media/207318/hmg_security_policy.pdf)

## Compliance

### Staff Responsibilities and delegations

HMRC should be proud of its achievements in raising understanding of, and compliance with, information security and assurance. As highlighted previously, HMRC has created a range of roles with specific information management and information assurance responsibilities, but there is a lack of clarity surrounding these roles.

Information Champions are appointed by each Director General to act on their behalf to oversee and co-ordinate action to assess and address information risks. They have responsibility for information governance within their business units, including the Data Guardian and Information Partner roles. The Data Guardian role is well established and was set up in as part of work to improve data security. Information Partners are tasked with ensuring business compliance with all relevant information related legislation and associated policies.

The importance of good KIM was not always fully understood, and, in some cases, management support beyond assigning the role to an individual was minimal. The majority of these roles are in addition to the substantive job, which can limit the available time and motivation to fulfil this role.

**Recommendation 30: HMRC should ensure that the individuals' assigned KIM roles are given the appropriate amount of time and support to meet their KIM responsibilities.**

### Policies and Guidance

KAI has worked hard to develop, publish and update its information and records management policies and guidance on the Intranet. This was found to be useful and relevant to experienced KIM staff. However, other staff

perceived the guidance to be too complex for those not in specialist KIM roles. Additionally, multiple versions of the guidance were available, leading to confusion as to which was the definitive version.

**Recommendation 31: HMRC must exercise control over business areas when they adopt, amend and publish KAI policies to ensure that only the latest versions of the policies are utilised.**

## **Training**

Training on information management is via an online e-learning package introduced in December 2009, which had been accessed by a total of 37,017 staff by March 2010. Most staff interviewed had heard of or completed the online training package prior to the IMA and felt it offered a good basic introduction. KAI has actively championed the package across the department and HMRC should be commended for this.

A broad indication of the level of understanding of KIM across the department can be gained from the results of the KAI Records and Information Management Surveys. These were conducted in 2009 and 2010 and show a percentage increase in respondents who said they knew what information to keep, where they should keep it and how long they needed to keep it for. This increase may in part be due to the roll-out and wide uptake of the e-learning package, the contents of which were likely to be fresh in the minds of many who took part in the 2010 survey.

HMRC needs to ensure that virtual learning is backed up with local activity in support. For instance, staff within the Benefits & Credits directorate (B&CD) approached virtual learning as a team exercise with meetings to discuss related issues. The staff handbook and posters were used to reinforce the information security message. This method could be used to promote the KIM e-learning package and the message that well-organised information underpins information security.

**Recommendation 32: HMRC to provide supplementary material to support the KIM e-learning package or incorporate this into the Data Security Handbook.**

HMRC provides formal classroom training on data security as part of the induction process but not on KIM. Instead, HMRC relies mainly on e-learning and local training of staff. KAI delivers some events and attends meetings, as resources allow, but as part of their “raising awareness” efforts and not as part of the induction process. HMRC acknowledges that making new entrants familiar with sound records and information practices would be of benefit.

**Recommendation 33: HMRC should include KIM training within induction training for new staff.**

HMRC has invested resources in KIM roles within the department, but how these roles are filled, used and developed has been left to the discretion of individual business areas. At the time of the assessment there was no training available for these roles.

**Recommendation 34: HMRC should implement appropriate KIM training for each of the specific departmental KIM roles.**

## **Change Management**

Senior management constantly referenced the “journey” that HMRC is on. They recognise that change is needed to create a leaner, more efficient and effective department. The Pacesetter programme, which will eventually cover all HMRC, encapsulates how this will be achieved. Pacesetter initiatives have two main themes: business change and capability delivery. The latter focuses on management and delivery process, mindsets and behaviours (“Lean” principles) and is underpinned by a drive to develop management capability. Staff members interviewed were highly complimentary of the programme.

Benefits & Credits is working with the Future Pacesetter team to introduce IM principles into the existing Pacesetter tools (7 Wastes and 5 Ss) and they are

being integrated into the PaceSetter learning syllabus, PaceSetter roadmap and Blueprint.

HMRC should consider incorporating KIM principles and governance as part of the programme to demonstrate how KIM can benefit and improve the way that HMRC operates.

**Recommendation 35: HMRC should incorporate KIM into Pacesetter principles to support raising the awareness and the benefits of KIM across the department.**

## **Culture**

### **Commitment**

HMRC is a large, dispersed department. The legacy of the merger of Customs and Revenue was frequently mentioned: when asked about their experiences within HMRC, staff often did so unprompted from a Customs or Revenue perspective. Most staff members have very specific tasks and do not see the potential to share information beyond traditional boundaries. Programmes such as Pacesetter, that operate across departmental silos and assist in identifying common processes, will provide opportunities for better information sharing.

HMRC has demonstrated KIM leadership and direction from the top. The Assessment Team also interviewed many engaged and committed operational staff who understood that good KIM practice can help them work effectively. However, there was a perceived gap in commitment, knowledge and support at the middle-management level. These managers were largely focussed on meeting their business or directorate objectives, without considering the impact of how their lack of engagement on KIM was interpreted by staff. The support of middle managers, leading by example, is essential in setting standards.

**Recommendation 36: HMRC should review and assess how to engage middle managers in supporting the KIM agenda.**

### **Knowledge Management/Transfer**

There is no formal or routine process for capturing the knowledge held by an individual when they leave. An individual's experience is important, especially in times of change. The Assessment Team were advised that the Legal Team have a process to capture an individual's knowledge as part of the exit process. In other areas it was ad hoc or non-existent. This is of relevance to HMRC as it continues its restructuring programme.

**Recommendation 37: HMRC should establish formal handover procedures to capture knowledge on internal transfer.**

There is some good practice in data sharing, for instance the Risk and Intelligence Service (RIS) in creating The Standard Intelligence Package (SIP) which provides a profile of a case with identified risks which is sent to local Compliance Offices. A recognised benefit of good KIM practice is that security profiles and staff vigilance become integral to day-to-day working.

There is no process for capturing or sharing the successes of the KIM programme or good practice stories. There is an opportunity to let staff across HMRC see the benefits of good KIM.

**Recommendation 38: HMRC should establish an online KIM space to capture and share examples of good KIM practice.**

## APPENDIX ONE: SUMMARY OF RECOMMENDED ACTIONS

This is a summary of the recommended action to:

- remedy the weakness identified; and,
- strengthen the commitment to the Information Management Assessment Programme.

These recommendations, when agreed, will form an Action Plan that will be monitored.

Business Area	Ref	Recommendation
Governance	1	HMRC should continue to invest in the structures that have allowed for significant progress on information assurance, and, more recently, management of information, particularly during this period of efficiency savings.
	2	HMRC should ensure that checking of compliance with KIM policies and standards is included as part of regular internal assurance processes.
	3	HMRC should develop a KIM performance measurement regime reporting to the SIRO.
	4	HMRC should better define the various KIM roles within the business, provide adequate support for those roles and improve communication of these roles to staff.
	5	Building on progress made, HMRC should take advantage of the Information Assurance programme, and now expand the agenda to include the benefits of good information management.
	6	HMRC needs to encourage staff to explore how they can maximise data flows to support delivery of its objectives while maintaining high levels of data security.
	7	Whilst The National Archives acknowledges the challenge in this complex information environment, HMRC should continue working to define key processes and their related information/data flows where relevant.

	8	HMRC should continue to improve its understanding of its key information assets.
	9	HMRC should harness the good work that has been initiated by local data integrity projects, sharing lessons learned across the organisation.
Records Management	10	HMRC should work closely with The National Archives and adopt the “What to Keep” guidance and approach.
	11	HMRC must introduce and implement appropriate retention schedules for heads of duty systems.
	12	HMRC needs to ensure that the owners of significant information assets are urgently identified at below Executive Committee level, agreed and assigned and that this is communicated appropriately.
	13	HMRC should ensure business areas rationalise and delete files on migration into CAFs, sharing good local practices to facilitate the process.
	14	HMRC to ensure that appropriate people with relevant skills are selected to fulfil the CAF Information Manager roles.
	15	HMRC should conduct compliance checks to ensure the integrity of the CAF creation and management process.
	16	HMRC to ensure that corporate guidance is followed and that all areas have approved retention and disposal schedules that are fully implemented.
	17	HMRC to implement a systematic approach to managing paper based records.
	18	HMRC should incorporate digital continuity into HMRC’s Gateway process for managing ongoing change.
	19	HMRC needs to engage with its supplier to clarify the contractual responsibilities for digital continuity and agree ongoing support in managing and maintaining digital continuity.
	20	HMRC should undertake a full impact assessment prior to any technological change that may affect the completeness, availability and usability of the department’s information assets.
	21	HMRC should undertake a limited review of BDAPs with respect to digital continuity in order to manage and mitigate the risks of these applications until a longer term solution has been agreed.

	22	HMRC to carry out assurance that all staff, including managers leading by example, adhere to the email policy and do regular “housekeeping” of their accounts.
	23	HMRC should develop information networks to share good practice across the organisation and build a professional community of shared interest in KIM.
Information legality	24	HMRC should clarify its guidance on how internal personal information should be managed to increase compliance across the department.
	25	HMRC to assess the validity of incorporating a review date in its Gateway memorandum of understanding covering use of its data.
	26	HMRC to monitor whether data is being used as prescribed in the Gateway Agreements.
	27	HMRC should identify what further information it can make available as part of the drive to open up public data.
	28	HMRC needs to further improve assurance of third-party contractors.
	29	HMRC to reinforce the usage of the Data Security Handbook’s guidance on Protective Marking to all staff.
Compliance	30	HMRC should ensure that the individuals’ assigned KIM roles are given the appropriate amount of time and support to meet their KIM responsibilities.
	31	HMRC must exercise control over business areas when they adopt, amend and publish KAI policies to ensure that only the latest versions of the policies are utilised.
	32	HMRC to provide supplementary material to support the KIM e-learning package or incorporate this into the Data Security Handbook.
	33	HMRC should include KIM training within induction training for new staff.
	34	HMRC should implement appropriate KIM training for each of the specific departmental KIM roles.
	35	HMRC should incorporate KIM into Pacesetter principles to support raising the awareness and the benefits of KIM across the department.
Culture	36	HMRC should review and assess how to engage middle managers in supporting the KIM agenda.

	37	HMRC should establish formal handover procedures to capture knowledge on internal transfer.
	38	HMRC should establish an online KIM space to capture and share examples of good KIM practice.

## APPENDIX TWO: IMA COMMITMENT

I am personally committed to making sure that we create and manage the information we need to fulfil our corporate obligations. To show the strength of my commitment, both in HMRC and to our partners, I have asked The National Archives to begin the process of assessment. The National Archives final report will be published.

I will provide effective leadership on Knowledge and Information Management capability across my Department. I will make sure that our internal processes and training support effective information management. Information is recognised as a key asset in HMRC and is used to support effective data and information sharing and knowledge creation. I will ensure that our information is appropriately captured, described, managed and preserved and that the risks are controlled. I will promote access to and re-use of our information, and protect personal and other sensitive information.

Permanent Secretary

## APPENDIX THREE: GLOSSARY

BDAP	Business Developed Applications
CAF	Controlled Access Folder
DPA	Data Protection Act
DRO	Departmental Records Officer
FOI	Freedom of Information
GKIM	Government Knowledge and Information Management
HMRC	Her Majesty's Revenue and Customs
IM	Information Management
IMA	Information Management Assessment
KAI	Knowledge, Analysis and Information
KIM	Knowledge and Information Management
PAYE	Pay as You Earn
RM	Records Management
SIRO	Senior Information Risk Owner