The National Archives

Information Management Assessment

HM Revenue & Customs

Reviewed

July 2016

Published

July 2017

Working with government
to raise standards in information management

Contents

Statement of commitment

In advance of each Information Management Assessment (IMA) we recommend that permanent secretaries publish a statement of commitment to the assessment process that also underlines the importance of good practice in information and records management. No statement of commitment was published in advance of the HM Revenue & Customs (HMRC) IMA reassessment.

IMA reassessment background

HMRC first underwent an IMA in 2010, which was formally closed in 2012. The reassessment of HMRC involved a detailed review of supporting documentation followed by interviews with senior staff, specialists and practitioners. These were held in the department's London offices between 4 and 7 July and on 10 and 11 July 2016. Additional interviews with key staff were conducted by telephone on 15 July 2016.

This report provides a summary of good practice and risks we identified. The central Security and Information Directorate and security and information specialist staff within divisions have responsibility for personnel and building security as well as information security. The former aspects are out of scope. IT and information governance within the Valuation Office Agency (VOA) are also out of scope. The VOA is only covered in terms of the basis on which responsibility for information management is delegated to the agency.

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

Glossary

CAF – Controlled Access Folder

DRO – Departmental Records Officer

FOI – Freedom of Information

HMRC – HM Revenue & Customs

IAO – Information Asset Owner

IMA – Information Management Assessment

IRM – information and Records Management team

KIM – Knowledge and Information Management

.pst – Personal Storage Table, format used for storing email

S&ID – Security and Information Directorate

S&IBP – Security and Information Business Partner

SIM – Security and Information Manager

SIRO – Senior Information Risk Owner

TB - Terabyte

VOA – Valuation Office Agency

Key findings of the assessment

1 The value of information

Key developments since the last IMA:
• HM Revenue & Customs (HMRC)'s Knowledge and Information (KIM) strategy has lapsed. At the time of the 2012 progress review we noted that knowledge and information management was being championed at board level. We saw no indication that this is still the case. Following its previous Information Management Assessment (IMA), HMRC set up a central Information Asset Register. This has since been abandoned.

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

- HMRC distinguishes between information and data, but has not formally defined what it means by either of these terms. Information and records management currently has a low priority. Security and IT strategies are in place, but the department has not established any strategic goals for information management to link to or support these documents. Without agreed objectives, the department's priorities have not been defined. No clear direction is being set for the central team or for devolved governance structures operating in lines of business.
- HMRC allocated the mandatory role of Information Asset Owner (IAO) at Director General level in the aftermath of the 2007 loss of two discs containing details of 25 million child benefit recipients. This decision has not been reviewed since. IAOs are delegating responsibility to support staff, but there is a limited framework in place to define how this happens and a lack of central mandate. In the absence of current policy or guidance and consistently used information asset registers, HMRC cannot have full knowledge of the information assets it holds or the risks they are subject to. As such, it is not in a position to meet key

requirements set out in the Security Policy Framework or in supporting guidance for IAOs.[1]

2 Digital information and supporting technology

Key developments since the last IMA:
• Since the 2010 IMA, HMRC has rolled out shared drive based Controlled Access Folders (CAFs) to all staff. A range of other systems including Google Drive are also available to staff.

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

- CAFs can be subject to greater levels of control than the unstructured shared drives that were in use at the time of the last IMA. Nonetheless, they do not meet the requirements for IT systems set out in the Section 46 Code of Practice. The amount of control exercised over them in practice varies. They offer no protection information with value beyond access restriction through permission lists, no technical restrictions on structure and no automation of processes for disposal. Current and legacy digital information is distributed across a number of locations, with large volumes held in personal drives and stored in vulnerable personal storage table (.pst) format. HMRC must take the opportunity to improve the situation offered by the planned introduction of a new IT platform.
- HMRC has limited knowledge of the age and format of the digital information it holds and it has not conducted a digital continuity risk assessment. It is not planning to ensure that it can continue to use its information in the way it needs, for as long as it needs, over time and through change.[2]

[1] https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework
[2] http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/what-is-digital-continuity/

3 Information risk, governance and oversight

Key developments since the last IMA:
• Information management governance is delivered by the central Security and Information Directorate rather than the Knowledge Analysis and Intelligence Directorate. A tiered governance board structure is in place under the main Senior Information Risk Owner (SIRO) Strategy Group. The roles of Data Guardian and Information Security Manager have been replaced as part of a move to introduce a new security operating model.

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

- An information and records management related risk has been drafted, which will have visibility at SIRO level once finalised. We also saw evidence that some security and information specialist staff had defined risks related to compliance with corporate policy at a local level.
- HMRC operates a tiered board structure under the main SIRO Strategy Group. This offers a potentially solid framework for oversight of information related issues. However, data is not currently within scope of these arrangements. While there is scope for IT staff to be called in as experts, they are not included in the standing membership of the SIRO Strategy Group or the supporting Information Management Group. In our view, both points undermine the department's ability to arrive at a single coherent view of what needs to be done.
- In addition, while it is positive that HMRC recognised the need to overhaul its devolved networks and redefine and professionalise support roles, new arrangements are yet not embedded. We are particularly concerned to note the limited degree to which information and records management has been factored

into the new model. We saw limited indication that the relationship between the centre and lines of business in this regard had been fully defined, with little evidence of routine consultation of the centre or of minimum mandated standards being defined and adopted.

- In the absence of a current information management policy, HMRC was not providing any central mandate on required processes and behaviours. This was addressed following the IMA with the publication of a new policy on GOV.UK.[3] This is in line with recommendations made in Sir Alex Allan's 2014 *Records Review* report.[4] Now that this has been done, HMRC must ensure policy obligations are acted on consistently by lines of business. Greater control is needed of the creation and application of retention schedules. To date, HMRC has not been able to meet the additional recommendation made by Sir Alex Allan that departments should also publish retention schedules, providing greater transparency on their decisions on records retention and disposal.
- HMRC delegates responsibility for ensuring and monitoring compliance with policy to lines of business. These are expected to define and develop their own assurance programmes. In our view this is inappropriate. HMRC does not know the extent to which policy and guidance is being followed and needs to put in place a centrally directed process to assess this.

4 Records, review and transfer

Key developments since the last IMA:
• HMRC is currently transferring no records.

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

[3] https://www.gov.uk/government/publications/hmrc-records-management-and-retention-and-disposal-policy

[4] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/370930/RECORDS_REVIEW_-_Sir_Allex_Allan.pdf

- HMRC has limited oversight of the paper and digital records that it holds. This is a key factor in the information confidentiality, availability and integrity related risks that HMRC faces. The likelihood of these risks occurring will be increased by HMRC's forthcoming programme of office closures. Controls need to be put in place to address this.
- Appraisal reports developed by lines of business after the previous IMA have not been revisited since and HMRC is only selecting a narrow range of files for permanent preservation. The destruction of digital information is occurring on an inconsistent basis across the department as a result of central pushes. Engagement from the business is varied. CAFs are likely to be difficult to review where orphaned or complex in structure. It is unclear how many business areas have fully defined, accurate and well communicated retention schedules in place. HMRC last transferred records in 2012 and has not yet begun to define processes for digital sensitivity review and transfer.

Recommendations to address risk areas

Recommendation 1
Define an HMRC strategy for knowledge and information management
This would be supported by: • ensuring that all information, both customer and non-customer, physical and digital, is included in the strategy • aligning the information strategy with IT and security strategies and any separate data strategy • learning from the example of other Information Management Assessment (IMA) programme members who have made significant progress in relation to knowledge management • ensuring that outcomes for more effective exploitation are defined, including internal and external re-use and improved performance under the Freedom of Information Act • ensuring the proposed annual reporting to the Executive Committee provides a summary of progress to deliver strategic goals

Recommendation 2
Establish clear and enforceable principles for information asset governance
This would be supported by: • producing guidance and policy that sets clear expectations for Information Asset Owners (IAOs) and security and information specialist staff • providing a clear definition of what an information asset is and how this definition should be interpreted and applied • introducing a mandated Information Asset Register template and telling staff how it should be used • reviewing the level at which the IAO role is allocated • factoring information management into IAO assurance

Recommendation 3
Identify key priorities for improving information management practice and culture and driving business engagement
This would be supported by: • as a priority, defining what ‘good’ looks like for information management and setting clear expectations for staff, managers and senior employees in relation to records creation and storage

- in conjunction with this, putting in place a defined process by which compliance within lines of business must be monitored and reported
- defining why information management matters, and why time and resource need to be devoted to it, and promoting this message
- gaining senior support for tackling identified priorities and necessary work that needs to be conducted within lines of business
- ensuring that knowledge and information management is included in induction training
- providing clear consistent guidance in relation to risk areas such as email, structure of Controlled Access Folders (CAFs) and use of alternative repositories such as Google Drive
- putting in place processes to ensure information management requirements are established for all new teams and projects from the outset

Recommendation 4

Ensure that the IT change enables the effective management, protection and exploitation of information

This would be supported by:

- giving consistent consideration to records management related requirements, including those for disposal, as a component of its procurement
- embracing the opportunities offered by new IT environments to enable better information management – gaps in requirements so far identified include:
    - the ability to set retention by information type or level of structure
    - long-term preservation (it must be possible for information to be reviewed and retention periods extended if necessary and it must be possible for information to be transferred or migrated to another system with that retention information preserved)
- including IT in the membership of information boards and defining how data management fits in to the current board structure

Recommendation 5

Gain greater oversight of legacy information in all formats to enable effective management and control

This would be supported by:

- ensuring that up-to-date, quality assured retention schedules are defined for all lines of business and easy to follow guidance is established on identifying information with value. Staff-led weeding and disposal activities should not take place unless staff are clear what they need to keep.

- developing a plan for managing information held in email, .pst files and personal drives
- formalising steps for the interrogation of CAFs by security and information specialist staff using existing tools
- developing a plan to increase oversight of paper and for the management of information identified through the office closure process
    - this should set out the timescales, required outcomes and specify key staff that need to be involved
    - the requirements of the Independent Inquiry into Child Sexual Abuse must be factored in
- working with The National Archives to revise and improve its process for the appraisal, selection and sensitivity review of paper files
    - The support of senior staff should be sought for this where lines of business need to be involved and allocate time and resource
- working with The National Archives to define processes for the appraisal, review and transfer of digital records.

Recommendation 6

Establish a definition of information and records management risk

This would be supported by:

- reflecting IT-related causes and mitigating actions in the final high-level risk description together with governance related considerations
- providing a central steer on ownership of compliance aspects of the risk within lines of business
- making specific reference to information management related risk in HMRC's information risk policy. This should include underlining legal and regulatory requirements and establishing the role of the Departmental Record Officer (DRO)

Recommendation 7

Strengthening current governance arrangements for information management

This would be supported by:

- giving information management more priority in the security operating model. It must:
    - define and launch required roles and mandate resourcing levels, including at an administrative level
    - put in place plans to engage and utilise security and information specialist staff to improve HMRC's capability
- reviewing the Terms of Reference of the Information Management Group and setting out its role within the governance structure in revised information risk and

information management policies

- strengthening the position of the DRO by formally defining how key responsibilities are delegated to Security and Information Business Partners
- reviewing the role of the central information management team to ensure they can be defined and established as a central expert resource
- ensuring the central information management team has a business plan in place that is aligned to the information management strategy and other relevant corporate documentation
- conducting an assessment of guidance that is published centrally and locally, and establishing clear processes for the production, sign off and review of guidance in the future
- clarifying how responsibility is delegated to the Valuation Office Agency.

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

Many of the staff we spoke to recognised in a practical sense the importance of protecting information. They also recognised the role that information management played in ensuring the availability of evidence and the security of customer records. This was particularly pronounced in teams with a significant business requirement in this regard. We were pleased to note that information management and information security related topics are included within the quarterly Key Management Actions assurance process. We gained a good level of assurance that managers were raising in meetings topics such as retention and disposal of information and management of Controlled Access Folders (CAFs). **This is good practice.**

However, at the time of the Information Management Assessment (IMA), the benefits that HMRC might otherwise gain from this and other information management related initiatives were undermined by the lack of a published information management policy. Without this, HMRC had no mandate or framework to drive compliance and build the required culture. We were supplied with a copy of a draft records management and retention and disposal policy dated January 2016. While it is positive that this has now been signed off, endorsed and publicly published, we note that it does not set out any of the business benefits to HMRC of good practice in information management or highlight any of the risks associated with poor practice. As such it only tells part of the story of why information management matters. The policy states that the central team is responsible for transferring records selected for permanent preservation to The National Archives and other places of deposit, and that:

> Lines of business are accountable for the management and disposal of all other records that they create.

It does not set out the specific responsibility of staff to create a record of their work and ensure it is stored appropriately. It also does not set out any specific requirements for managers or senior staff. This leaves the Key Management Actions without a policy basis and means that the policy provides no starting point from which to drive engagement with managers and senior staff.

We saw no indication that departmental capability in information and records management has been recently discussed at board level despite the current period of scrutiny of government department's performance in records keeping. There was little evidence of the top-down support for information management that Sir Alex Allan identified as necessary in his 2015 *Digital and Archives Review* report[5]. It was also clear that while security and information specialist staff in many areas are working hard to push information management priorities, key messages are not always being heard or acted on. One interviewee noted:

> Information management can be seen as a dry subject and buy-in is an issue – I think the value of information is understood and the need to protect information and access to it is recognised. Less so the need to devote resource [and time] to housekeeping … People need incentives and a management dictat – a clearer message on why this matters, such as the impact on storage costs.

Another stated:

> I would like a stronger centre steer that [information management] is vital. A stronger central steer is needed that this is a vital area – a 'must do' rather than a 'nice to do', and something with substantial benefit. Currently the whole agenda comes across as an add-on. A stronger push is needed, with time allocated.

HMRC must define more clearly why information management matters, and why time and resource need to be devoted to it. It should also clearly establish the roles of staff, managers and senior employees. Once expectations are set, HMRC needs

[5] https://www.gov.uk/government/publications/records-review-by-sir-alex-allan

to put in place a plan to drive business engagement and promote responsibilities. This will require the support of senior management **See recommendation 3**

Setting goals for information and its management

The HMRC security strategy was produced by the Security and Information Directorate, of which the information and records management team are part. The strategy is endorsed at non-Executive Director level and takes a holistic approach to security, covering people, process and technology. Information security is within scope and the document also touches on information management systems and functions, noting the need to ensure alignment with knowledge and information management and business continuity professions.

HMRC's publicly published IT strategy sets out the contribution of IT to the department's transformation programme and vision and to individual directorate business plans.[6] The strategy highlights plans for HMRC's three core tax administrations and five cross-cutting platforms, including the removal of legacy applications. Potential improvements in relation to information security and information and records management are both identified. Under the heading of Enterprise Content Management, the strategy sets out plans for the introduction of content management tools and improved lifecycle management together with greater digitisation of paper and microfiche records.

There is no information and records management strategy and we saw no evidence that strategic goals for the management or exploitation of information and records had been defined elsewhere. Neither the IT strategy nor the security strategy are therefore supporting and enabling any defined and agreed set of outcomes. At the same time, there is no strategic vision that establishes how good practice in information and records management will help the achievement of expected benefits from new technology or support security related outcomes.

Additionally, HMRC lacks a current strategy for knowledge management and exploitation. The senior staff we spoke to were clear that risks relating to knowledge

[6] https://hmrcdigital.blog.gov.uk/wp-content/uploads/sites/20/2016/02/HMRC-IT-Strategy-2016.pdf

loss in the context of HMRC's transformation programme are recognised and have been discussed at the highest level. However, we saw no evidence that a consistent approach to knowledge capture and knowledge management is yet in place. We recommend that HMRC should learn from other IMA programme members that have conducted significant work (and made significant progress) in this area.

HMRC is undergoing a significant period of organisational change. It is half way through a ten-year transformation programme that aims to create a tax authority fit for the future. In this context it needs to address as a priority the current gaps in its provision of information and knowledge-related strategy, defining how these will support achievement of HMRC's overall vision. We recommend that HMRC establishes a holistic vision for its knowledge and information, defining clear strategic goals for the management and exploitation of both. **See recommendation 1**

HMRC's obligations as a public records body are established in the Public Records Act.[7] This makes no distinction in terms of information format or means of transmission. We therefore recommend that goals for lifecycle management cover both physical and digital information. This should include customer and non-customer information. It is particularly important to establish clear goals in this area in view of the recent separation of governance responsibilities relating to information and data between the Security and Information and the Knowledge Analysis and Intelligence directorates, as discussed below (see p. 28).

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

HMRC runs a devolved system for handling requests for information under the Freedom of Information (FOI) Act. Requests come in centrally and are then passed out to the lines of business. The team of four FOI advisors provides advice and support to the business to answer the requests. There is limited provision for tracking the progress of FOI requests, although plans are in place to introduce a case management system.

[7] http://www.nationalarchives.gov.uk/information-management/legislation/public-records-act/pra-faqs/#pub-bodies-duties-pra

Latest available statistics at the time of the IMA show that HMRC received 565 FOI requests in the first quarter of 2016.[8] This is the third highest volume among monitored organisations that are not departments of state and the eighth highest overall. Of these, 85% were answered within 20 days or permitted extensions. 85% is the minimum standard set by the Information Commissioner's Office (ICO); performance below this may initiate a period of formal monitoring . HMRC's performance fell beneath this level for two quarters in 2015. Most of those organisations receiving a similar or higher number of requests performed better than HMRC. The percentage of resolvable requests granted in full was below average and the percentage of resolvable requests withheld in full was above average.

We were given verbal assurance that an FOI improvement plan has been put in place with a working group to drive it. HMRC should support this by ensuring the links between good information management and improved FOI performance are defined. **See recommendation 1**

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

HMRC has no current central guidance on the governance of information assets or on the responsibilities of Information Asset Owners (IAOs). Its 2012 IAO handbook was not updated after the decision to move away from a centrally hosted Information Asset Register and is no longer hosted on the department's intranet. As such, HMRC is providing no definitive corporate steer on what should be identified as an information asset or how IAOs should discharge their duties. HMRC needs to ensure that proportionate coverage is given to information in all formats (not only customer information) and that information availability and integrity-related risks to information assets risks receive scrutiny in addition to confidentiality-related risks.

[8] https://www.gov.uk/government/collections/government-foi-statistics

While we were told that there is an expectation that lines of business should maintain information asset registers, without policy or guidance HMRC is providing no formal direction on this point. In a number of locations we visited no Information Asset Register was in place. HMRC is not in a position to meet requirements set out in its own internal Governance and Compliance policy, which should underpin the provision of annual statements of internal control. HMRC can have no confidence that current arrangements allow it to know what information assets it holds or the risks that they are subject to.[9] It is in no position to meet the requirements of its own Information Assurance and Risk policy, which states that information assets will be identified and risks will be assessed. Without a working information asset governance framework, statements in the records management and retention and disposal policy relating to delegation of responsibility for information management through IAOs are little more than aspirational.

HMRC must review current arrangements and establish clear agreed and enforceable principles. It must formally define what an information asset is and establish how it should be applied to both structured and unstructured information. Drawing on good practice examples developed by other IMA members, it should establish how IARs should be populated. **See recommendation 2**

Ownership of information assets

HMRC has allocated the mandatory role of IAO at Director General level, the same level at which the Senior Information Risk Owner (SIRO) role is allocated. Directors General have not received any training to enable them to discharge their responsibilities. Those we spoke to did not necessarily recognise that they held the IAO role and appeared reliant on the assurance processes put in place by the security and information specialist staff operating in lines of business (see p. 29). There is a risk that these may in some cases be based on well-established

[9] Plans to introduce new information security arrangements for government do not currently impose any changes on the frameworks that departments are expected to put in place for governance of information assets.

assumptions, which are not being challenged in the absence of an active corporately driven approach for the identification and cataloguing of information assets.

While the delegation of duties is fully within scope of published guidance on the mandatory role of IAO, HMRC is not providing the required steer to ensure this is being done consistently or along required lines.[10] HMRC should review the IAO role, the level at which it is allocated and the way in which responsibility is delegated with a view to either solidifying current arrangement or imposing new ones. Annual assurance provided by IAOs should be expanded to include information and records management. **See recommendation 2**

[10] https://www.gov.uk/government/publications/information-asset-owner-role-guidance

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

HMRC's current IT environment raises a number of significant challenges to its ability to capture and keep information as long as it needs.

CAFs do not meet the requirement set out in the Section 46 Code of Practice for the routine application of records management processes by IT systems. This includes the automated deletion of specified information in accordance with agreed disposal dates. CAFs were not set up to deliver this functionality and do not offer the facility to allocate retention schedules at folder level or otherwise. In addition, CAFs offer no protection from accidental or unauthorised alteration, copying, movement or deletion and do not meet Section 46 requirements in this regard. The compliance burden is therefore entirely on HMRC staff and the security and information specialist staff that operate within lines of business.

The situation is complicated by the availability of other shared repositories, including legacy SharePoint sites, an Electronic Document and Record Management system (Documentum) and newly introduced Google tools such as Google Drive, which has been rolled out to all staff. HMRC Google Academy branded guidance states:

> if your current information exists in a CAF or in SharePoint and you want to get the benefits of Google Drive, you should transfer the information, share it appropriately and delete the original information. We do not want multiple copies of the same information in several repositories.

Without third party plug-ins to extend Google Drive's functionality, the system offers no benefit in terms of lifecycle management over CAFs. In practice, information with

value stored in this environment is more vulnerable to loss because Google Drive is specifically intended as an enabling space for current and active work only (see p. 41).

The ability of staff to store information outside shared repositories is also a concern. Although limits are in place on email accounts, which is an important first step in encouraging capture of email in shared corporate areas, staff indicated that these could be expanded relatively easily. Personal drives are also accessible and are being used for storage; figures provided to us in advance of the IMA show that (as of October 2015) HMRC held a total volume of 54 TB of information in personal drives, a volume equal to that held in CAFs.

On this basis, the current IT environment places significant limitations on HMRC's ability to manage information in accordance with its value and on its ability to protect and exploit it. In the short term, HMRC must ensure that acceptable governance-based and technical mitigations to the risks raised by the IT environment are in place. It also needs to ensure that it secures the best possible solution for future management of its information as it moves to a new IT platform. While new platforms may offer increased enterprise search capability, this by itself will not be sufficient to address the risks that HMRC faces. **See recommendations 3, 4 and 5**

Finding, accessing and protecting information

Access to CAFs is controlled by email distribution lists that staff should be added to and removed from as required. These are overseen by managers in their capacity as CAF owners rather than by HMRC's security and information specialist staff, who need to be put on to distribution lists in order to have access to them. While a number of our interviewees felt this process ensured people had access to the information they needed, managers need to invest time and effort if it is going to work well. As one interviewee noted:

> In theory if people leave they should come off but people move all the time. Access should be by distribution lists but it's a [considerable] burden.

The staff we spoke to tended to work in and search for information in their own CAFs and did not look for information more widely. Nonetheless, the limited search functionality within CAFs increases the importance of adhering to sensible filing structures and naming conventions. While a good practice process exists to guide the structure of CAFs this is not automated and is not policed as a matter of course. As a consequence there is no constraint on the depth of structure for complex CAFs, which may impact on the ability of teams and the organisation to find information as needed. If staff do not believe information will be available as needed it provides a reason to retain it in email accounts and personal drives, where it will be accessible to the individual but not the organisation. HMRC should reinforce guidance on the structure of CAFs and use of naming conventions. **See recommendation 3**

HRMC's has a significant legacy of .pst files, with (according to October 2015 figures) 4.4TB held in CAFs and 12TB in personal drives. These files enable large volumes of information to be stored in a compressed format, from which it is easy to export large amounts of data, raising obvious information security concerns. Emails stored in this format may also be less stable and more subject to corruption. HMRC should put in place a specific plan to address this legacy. **See recommendation 5**

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 format and age

HMRC has limited knowledge of the age and format of its information and the locations in which it is held. Interviewees were not clear whether the estimated 20TB held in shared drives consisted of information or software and software files. The oldest information known about by the central team within the CAFs dates to 1999. Views of interviewees on the age of digital information held varied from the mid 1990s in one case, to 2010 when CAFs were introduced. In terms of the latter, one interviewee stated that any of their team's information older than 2010 would be held in personal drives and/or pst files.

Some security and information specialist staff have utilised a CAF structure analyser tool to assess folder size, age, ownership as well as folder structure and depth. Guidance produced by one business area indicated that the tool was being used to ensure the digital continuity of information stored in CAFs that needs to be retained beyond the standard retention period of 6 years plus 1.

While positive, these arrangements do not appear to have been adopted consistently by all lines of business, and where they have been adopted do not appear to be part of a systematic, centrally driven plan. They also do not cover any legacy information retained outside CAFs, such as personal drives and email. HMRC needs to gain greater understanding and control of its legacy digital information and should establish this as a key objective in its information strategy, learning lessons from IMA programme members. It should formalise steps to be undertaken by security and information specialist staff in relation to interrogation of CAFs utilising existing tools, embedding good practice and lessons learned. **See recommendation 5**

IT change

The 2010 HMRC IMA report noted the issues caused by its reliance on bespoke and legacy applications and IT systems, including heads of duty systems that were not set up to enable disposal of customer data. We gained a good level of assurance that HMRC is actively seeking to migrate away from aging technologies and embrace open source technologies. HMRC must ensure that the Departmental Records Officer (DRO), central Knowledge and Information Management (KIM) staff and IAOs are fully engaged with this work. HMRC needs to do more to ensure that information and records management related requirements, including those for disposal, are considered as a component of its procurement process that is delivered by the Architecture Review Board and Technical Design Authority. **See recommendation 4**

Key context for this IMA is the expected introduction of HMRC's new IT environment. We saw little evidence of proactive collaboration between IT and KIM staff on the development of business requirements and note that information and records management requirements form a small percentage of the whole.

HMRC should ensure information management requirements are reviewed in light of this report, to ensure they are adequate. Key gaps should be addressed, including the ability to identify record content and the provision of central oversight. We note that the following have not been referenced in the requirements HMRC has defined for its new system:

- the ability to set retention by information type or level of structure
- long-term preservation (it must be possible for information to be reviewed and retention periods extended if necessary and it must be possible for information to be transferred or migrated to another system with that retention information preserved).

HMRC must address these points. It should ensure that the new IT environment delivers these requirements and that sufficient resource is applied to the design, configuration and roll out of the new system. **See recommendation 4**

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

HMRC has defined at a strategic level the potential impact of cyber security related risk. We were not shown a risk description but understand that the risk has been positioned to reflect and give priority to a number of different categories of potential cyber attack and threat.

An information management related risk was defined at Executive Committee level under HMRC's previous joint governance arrangements for information and data. At the time of the IMA, a new draft risk description had been produced, which was going to be sponsored by the SIRO. No mitigating actions had yet been defined, but we are pleased to note that positional text for the draft highlighted the need to feed in findings from the IMA reassessment.

The draft information management risk description highlights a number of potential outcomes including financial loss, reputational damage and missed opportunities to exploit information. It does not explicitly reference compliance with the Public Records Act or state that information management failures might undermine business effectiveness and efficiency. It does not fully set out the impact if HMRC could not establish the basis on which past decisions had been taken. Identified causes focus on failures in the application and provision of policy, the limitations of the current IT environment and the resource intensive nature of processes.

HMRC was due to discuss the risk at an Information Management Group meeting (see p. 27) following the IMA and at an internal Information Management Risk review workshop. HMRC now needs to sign this risk off and monitor progress to control it. HMRC needs to ensure that IT related causes and mitigating actions are reflected in

the final agreed risk description together with governance related considerations. **See recommendation 6**

Implementing an information risk management approach

We were told that HMRC's SIRO Strategy Group is intended to provide active scrutiny of information and security related risks. One senior interviewee described its objectives as follows:

> To keep information and security requirements on the agenda with nowhere to hide and get a cadre of senior business representatives around the table. It adopts a thematic approach looking at areas like cyber or supplier security. The aim is to raise standards and [it is] doing well in terms of getting people engaged.

This strategic level body is chaired by the SIRO and supported by five management boards including the Information Management Group, which is chaired by the Director of Information and Security. This arrangement provides a potentially effective route for escalation of information and security related risks up to Executive Committee level. This will include risks relating to information management once the department has formalised its risks description and identified its risk appetite.

We saw positive indications that HMRC is actively using the Departmental Security Health Check process to engage lines of business on key information risks, including those relating to information management. We also saw positive indications that information management risks were being defined at a local level by some security and information specialist staff, with interviewees from one line of business stating that risks relating to retention policy and CAF usage had been logged on their risk register. Once the wording of the main information management risk has been finalised, HMRC should provide a central steer on ownership of key aspects including relevant mitigating actions. **See recommendation 6**

To enable this, HMRC should ensure that its information risk policy, which was being reviewed at the time of the IMA, makes specific reference to information management related risk. This should include underlining legal and regulatory

requirements and establishing the role of the DRO within risk management structures. **See recommendation 6**

3.2 Establishing control

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

Governance structures

At the time of the IMA, Terms of Reference for the SIRO Strategy Group had not been updated to reflect the May 2016 appointment of the department's new Director of Information and Security. They also still stated that the Group had strategic responsibility for data management, although this is no longer the case. However, we gained a good level of assurance that it has performed an active role, for example reviewing and approving plans for HMRC's new information security operating model in spring 2015 (see p. 29).

Terms of Reference for the supporting Information Management Group are also out of date. They have a next review date of June 2014, still carry the branding of its predecessor, the Information and Data Management Group, and do not reflect current information governance structures.

A February 2016 agenda supplied by HMRC indicates that a wide range of topics are scrutinised, from KIM professionalism and Google trials to progress of retention and disposal campaigns. Strategic topics such as the cross government records management project and HMRC's response to Sir Alex Allan's 2014 *Records Review* report were also in scope. HMRC needs to update the Terms of Reference of the Information Management Group and should ensure its role within the governance structure is set out in the revised information risk and information management policies. **See recommendation 7**

Since the decision to remove data management from the scope of the SIRO Strategy Group, no separate data management body has been established at the management tier. There is no dotted line into the Knowledge Analysis and Intelligence directorate, with which responsibility for customer information is shared by the Security and Information Directorate. HMRC should define how data management fits in to the current structure and ensure IT is represented among the standing membership of information boards. Without this, HMRC's ability to adopt a joined-up strategic approach for the management, protection and exploitation of its information will be undermined. **See recommendation 4**

Supporting the business

The HMRC Information and Records Management (IRM) team is based within the Security and Information Directorate (S&ID) and is headed up by the deputy DRO. Its remit is defined as follows:

> The IRM Team actively supports the DRO in leading on compliance with the Public Records Act and the management of HMRC information, including maintaining the statutory relationship with The National Archives. The team also provides input to projects that directly support the DRO in discharging their responsibilities and provides direction to other teams in S&ID to ensure they practice good information governance.

The team should be five strong, which is small for a department of HMRC's size, but had a headcount of two at the time of the IMA. The team is defined as a second line assurance function. Though working proactively, its ability to fulfil this function was limited at the time of the IMA by a number of factors including the lack of an information management policy and absence of compliance monitoring processes (see p. 34). Although the deputy DRO has been instrumental in driving the agenda of the Information Management Group, the absence of an information strategy has in our view undermined the team's ability to plan effectively. We saw no evidence that the information and records management team has a current business plan. This must be addressed once strategic goals have been defined. **See recommendation 7**

In view of changes in reporting lines following the IMA, which are highlighted below (see p. 36), HMRC should review the team's remit to ensure it is best placed to deliver its function. A clear statement on the direction and service it provides to the business and to security and information specialist staff should be published and promoted internally. The team needs to be recognised as a central, expert resource that security and information specialist staff can consult. At the time of the IMA this was not the case and interviewees were not clear that they could or should ask the centre for advice and guidance on key questions. On one occasion we were asked for a steer on a long-standing retention-related query that did not appear to have ever been raised with the information and records management team. **See recommendation 7**

Support networks

The scale of HMRC and the small size of central functions such as the records management team necessitates the use of a devolved governance model. HMRC's previous information and security operating model was introduced in the aftermath of the 2007 disc loss. These were reviewed as an output from the HMRC security strategy. A March 2015 Executive Committee paper stated that the model had become fragmented and that the existing Data Guardian, Information Security Manager and Information Partner roles should be re-examined. The paper noted that there were differences in grades, resourcing levels and scope of accountabilities and responsibilities, reporting lines and governance across HMRC. In April 2016, the Data Guardian and Information Security Manager roles were replaced with the new positions of Security and Information Business Partner (S&IBP) and Security and Information Manager (SIM).

At the time of the IMA, new arrangements were not fully embedded. No role description had been produced for the strategic S&IBP beyond that which appeared in the job advertisement and security and information specialist roles were not yet established consistently in all areas. Based on our interviews, not all security and information specialist staff were clear what role they held, or appeared to have a business plan in place. Although proposals for the new governance model were raised at Executive Committee level, we saw no evidence of a concerted effort to

launch new roles and many interviewees (including those who held them and board level staff) continued to refer to the old positions.

In view of the issues noted in this report, it is clear that the previous governance model did not support HMRC in meeting its obligations in relation to the Public Records Act. The introduction of the new model with roles filled on a full-time dedicated basis and with central support for professional development has some potential to considerably improve the situation. However, we saw little to indicate that information management requirements had been identified as a core consideration and actively factored into plans. An opportunity to give information management a firmer footing appears to have been missed.

At the time of the IMA, the Information Partner role had not yet been reviewed and as a consequence continues to be resourced inconsistently. Widely differing interpretations of the role were evident through our interviews. Although the role still exists, there was no reference to it in the SIM role description. Guidance for the Information Partner role itself had also not been updated to reflect the introduction of the S&IBP and SIM roles or to clarify responsibilities for the time being. We saw no evidence of concrete, communicated plans for the Information Partner role.

SIMs and Information Partners interviewed highlighted the part-time role of Information Managers within teams. Both appeared reliant on Information Managers to carry out a range of key information management-related tasks. However, we saw no guidance for this role or reference to it in the paper produced for Executive Committee. We also saw some evidence that in some areas the role is not being resourced. One interviewee who sat outside the corporate centre stated:

> Information management is seen as a nice to have rather than a must have – practically, resourcing and time spent are seen as negatives in the business context. Information Managers do half a day a week – they are getting squashed by managers and having to push back. If they aren't pushing back … there will be an impact on information availability … There is an emphasis on getting money in the door, but ignoring information management is a false economy.

Finally, we note that the job description for the new SIM role itself makes minimal and selective reference to information management requirements. These are not specifically mentioned in relation to SIM accountabilities to IAOs or to the Security and Information directorate. Where information management requirements are highlighted, they refer only to use of CAFs rather than the broader application of good practice information management principles.

HMRC is not setting a clear direction for its security and information management specialists in relation to information management related requirements. HMRC needs to give information management more priority within the new governance arrangements. It must define and mandate required roles and resourcing levels, including at an administrative level. It needs to put in place plans to engage and utilise security and information specialist staff to improve HMRC's capability. **See recommendation 7**

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

HMRC publishes a range of information management related guidance on its intranet. This does not appear to be easily accessible. A number of the staff we spoke to said they felt guidance was hard to find; page headings in screenshots supplied to us indicate that it is hosted five levels below the main intranet front page. On the basis of sample guidance supplied to us for review, content does not appear to have been reviewed to reflect the launch of the S&IBP and SIM roles; the information management pages also still contained links to help staff find their Data Guardian and Security and Information Manager as well as their Information Partner.

Individual lines of business are permitted to produce their own guidance where there is a specific business need. We saw no indication of a central process to govern its creation and, as a consequence, its quality is likely to be variable and to produce inconsistent practices across HMRC. Now that HMRC has signed off its records management and retention and disposal policy, it must review the guidance it publishes centrally and locally, ensuring clear principles are in place as it moves to introduce its new IT environment. **See recommendation 7**

What to Keep

HMRC has defined a standard retention period of six years in addition to the current year. The records management and retention and disposal policy states that lines of business are responsible for producing and publishing their own retention schedules.

We understand that a benchmarking exercise took place in 2011 after the department's previous IMA, which established that all lines of business had retention schedules in place. HMRC has not revisited this exercise since and does not know if this remains the case or if those that are defined are of sufficient quality. To date HMRC has been unable to meet the recommendation in Sir Alex Allan's *Records Review Report* that all departments should publish retention schedules.

We saw no evidence that the potential historic value of information is being considered up front as new key work streams and teams are established. It was clear from our interviews that a number of business areas have complex retention requirements that have not yet been defined. A sample retention schedule submitted to us for review set out a number of derivations from HMRC's standard retention period, including records of possible historic interest and records held for precedent purposes. No detail or context was provided to help staff identify this type of record, in contrast to other classes of record identified in the document. In addition, the review point was identified as 25 years after creation, suggesting that these record types were either added before the transition period to the 20-year rule began in 2013, or without knowledge of or reference to it.

Many of the staff we spoke to recognised a need to capture records within CAFs and a number had clearly defined processes in place to govern what needed to be

captured and at what point. This was by no means standard, however, with one interviewee for example describing ‘a myriad of CAFs and a lack of control with everyone doing their own thing’.

We saw low recognition of the potential long-term value of information among senior staff even where their staff were engaged in strategically important work streams. In general terms it was clear that many staff are keeping information on a ‘just in case’ basis, either from a lack of knowledge of how long information needs to be kept or a belief that defined retention periods are not appropriate. This, together with a lack of trust in the ability of CAFs to ensure information availability, is likely to be a significant factor in the volume of HMRC’s information that is stored in personal repositories. One interviewee stated:

> Do people keep things on a just-in-case basis? Yes people do and I do. From my perspective, the same things will be in email and in CAFs. It is easier to find in email and if you put it in a CAF you will forget it is there.

Another interviewee stated:

> I am close to the limit on my inbox. I have a great array of personal folders. I have kept a lot of stuff: sometimes it’s useful to prove that people have or haven't done something

HMRC must ensure it embraces the opportunities offered by the new IT environment to ensure the process of record creation is made as easy as possible for staff. It must also ensure that up-to-date quality assured retention schedules are established for all lines of business. **See recommendations 4 and 5**

Providing training

HMRC does not offer information and records management training as a component of staff inductions. **See recommendation 3**

3.4 Measuring impact

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

Measuring compliance with policy

The Section 46 Code of Practice recommends that information management policies should indicate how compliance will be monitored. HMRC's draft records management and retention and disposal policy states that:

> Lines of business are accountable for developing their own assurance programmes to ensure that the core principles in this policy are being complied with. Line of business retention policies and retention and disposal schedules should be reviewed on an annual basis.

We saw no evidence that any such processes are in place or that the central team or senior staff are clear how well HMRC is managing its information. While we recognise that some aspects of information management were highlighted in HMRC's Departmental Security Healthcheck, this was a small component of the whole and did not amount to in-depth scrutiny across all lines of business against a specified set of criteria. It is also unlikely that necessary levels of insight will be delivered by compliance checking activities conducted for the Key Management Action process, as information management again forms a small component of this and the process is focussed on staff awareness at a team level. Assessments are being made of how information is managed in CAFs, but arrangements appeared to vary widely. Although security and information specialist staff in some areas were setting out clear, auditable criteria in this regard, we saw indications that in other cases such work was merely a 'temperature check' or something that would get pushed to the back of the queue if more pressing team priorities arose. We saw no evidence of a centrally driven plan to conduct these activities or utilise outputs and note that these would in any case only cover a portion of HMRC's information holdings in terms of format and location.

HMRC needs to define what ‘good’ looks like for information management, establishing maturity criteria against which performance of the business can be measured, following the example of other IMA programme members. The process for monitoring compliance should be mandated from the centre to ensure a consistent view can be obtained. **See recommendation 3**

Assessing progress against strategic goals

We support the requirement identified in the draft records management and retention and disposal policy for an annual Information and Records Management progress report to the Executive Committee. This should be directed towards delivery of information goals once these are defined. **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

The DRO has a reporting line through the Director of Security and Information to the SIRO. As such, the role appears well positioned within wider systems of corporate governance, as recommended in guidance published by The National Archives.[11]

Since the IMA, the deputy DRO and information and records management team has been given a direct reporting line to the DRO. This positions them as a strategically rather than operationally and process-focussed team. We regard this as a positive move in view of HMRC's current low level of information management maturity. The change in reporting lines also means that the DRO is also now better positioned to meet requirements for the management, selection and transfer of records set out in The National Archives' guidance. In our view the position of the DRO would be strengthened by formally defining how key responsibilities are delegated to S&IBPs and their teams of security and information specialist staff. **See recommendation 7**

The means by which responsibility is delegated to information and records management staff within the Valuation Office Agency (VOA) should also be clarified as we understand no memorandum of understanding has been established setting out how responsibilities are delegated. This is particularly important as VOA, like HMRC, is not currently transferring records to The National Archives and lacks a signed instrument for the retention of public records. **See recommendation 7**

Oversight, control and use of records

[11] http://www.nationalarchives.gov.uk/information-management/manage-information/planning/departmental-record-officer/role-departmental-record-officer/

HMRC knows what customer information it holds in its Head of Duty systems, but has less understanding of the information that it holds elsewhere. This includes locations such as historic SharePoint sites, Google Drive and social media tools and information held in removable media. HMRC has set up a specific project to enable identification and destruction of the latter. It also includes the CAFs, which are likely to contain customer as well as corporate information.

While existing processes can help identify what CAFs exist and who owns them, available mechanisms such as the information asset governance regime do not support easy understanding of their contents and value. While some lines of business have put in place additional processes for the management of closed records, CAFs do not offer any means of differentiating information held within them on the basis of value other than manually. In some cases staff are adding phrases such as ‘do not delete’ or ‘keep for x years’ to CAF file lists or to folder or file names to try to highlight information with value. Where neither approach has been followed the value of the information they contain is likely to be unclear. As one interviewee stated:

> CAFs are just used as great big buckets. It is difficult enough to get [people] to name things properly – it would be hard to pull out anything [that had] worth.

As access is controlled by teams and teams are best placed to understand what is held, any loss of ownership is likely to make things more complicated. We saw evidence that orphaned CAFs already exist and the number of these may be increased by HMRC’s forthcoming programme of office closures and associated organisational change.

At the time of the IMA, HMRC’s paper records were stored by Iron Mountain and seven additional in-house facilities. Records held in Iron Mountain are tracked via the company’s accutrak system. HMRC lacks a system of its own for tracking paper records beyond an Excel spreadsheet. While there has been discussion of the need to procure a tracking system, no decision to do so has yet been taken.

HMRC does not have full oversight of the information that is held in its paper storage facilities locations, although spot sampling activities have taken place. There is no central understanding of the additional volumes of paper records that are held in the business over and above the small legacy discovered through a 2015 awareness campaign led by the information and records management team. Local oversight is variable and we saw no evidence of a defined attempt to address the situation beyond seeking options for low cost storage. This underlines the importance of ensuring physical records are in scope of HMRC's strategic information management goals. **See recommendation 1**

As with CAFs, the risks that this situation raises for HMRC are made more significant by the forthcoming programme of office closures. It needs to put in place controls to ensure paper records, and any information held in other forms such as yet undiscovered removable media, are handled appropriately, identifying a requirement for ongoing central storage where value is identified and putting in place arrangements for secure disposal where this is not the case. There are clear potential data protection and security related concerns if this does not take place. At the same time, if records are sent to central storage without clarity on their contents, HMRC will be creating a future burden in terms of review and disposal. An additional layer of risk is added by the requirement to retain any older records for the duration of the Independent Inquiry into Child Sexual Abuse (see p. 40).

On this basis, we strongly recommend that a forward-looking plan is developed for the management of information identified through the office closure process. This should set out the timescales, required outcomes and specify key staff that need to be involved such as the DRO, the central information and records management team and local security and information specialists. **See recommendation 5**

Appraisal and selection

Although appraisal reports are hosted centrally on the records management pages of the HMRC intranet, these have not been revisited since they were compiled in 2011. They had a low profile among the security and information specialist staff we interviewed.

We recognise that the information and records management team has contacted staff to ask them if they held information with potential historic value. In our view though, security and information specialists and staff lack guidance to appraise value accurately.

The lack of insight that HMRC has into its historic records is evident from the fact that HMRC's entry in the autumn 2015 Records Transfer Report reports only 37 records held for the period 1987-8. Of these, 7 are identified as having historic value. A total of 18 records are identified for the period 1989-90, of which HMRC plans to transfer 7. Both sets consist of bound finance bills. This is across both of HMRC's predecessor organisations. This seems a very low number of records for an organisation that today highlights the vital role it delivers in enabling the UK's public services and helping families and individuals with targeted financial support. HMRC staff have given their view that there must be more records that could be selected; as yet no means of doing so has been established.

Working with The National Archives, HMRC needs urgently to reconsider and improve its process for the appraisal, selection and sensitivity review of paper files. HMRC needs to provide the senior support necessary to progress this work where lines of business need to be involved and allocate time and resource. HMRC should explore a macro approach where possible and document its selection criteria either through developing an Operational Selection Policy, revised appraisal reports or similar mechanism. **See recommendation 5**

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

To meet the requirements of the Independent Inquiry into Child Sexual Abuse, HMRC has ceased to destroy paper records in its central repositories that are older

than their due retention date. HMRC has stated that any paper records falling into this category discovered outside these locations should be retained and retention schedules should be amended accordingly. In contrast to the stance adopted by a number of other Whitehall departments, it has opted to continue normal business as usual disposal of paper and digital information that fall due at the normal retention date. Staff locating any such records are expected to retain it for the duration of the inquiry and amend retention and disposal schedules accordingly. This decision has been communicated at Executive Committee level, in line with guidance provided to departments by The National Archives that senior approval should be sought.

We saw evidence of a number of disposal focussed initiatives run by information specialists, including a 2015 Outlook Housekeeping exercise. Interviewees in particular referenced the 2015 'if you don't need it – delete it' campaign that was promoted by the Education and Awareness team within the Security and Information Directorate. This was implemented locally by information specialists. One interviewee described their process as follows:

> We asked the IT team to provide a spreadsheet that includes the size of the CAFS. We looked at [the numbers] again at lunchtime and at the end of a day to see how the size has changed. It creates a bit of competition … the top line is get rid of as much as you can.

This kind of manual approach to digital disposal is necessitated by the fact that CAFs do not support automated disposal, as noted above (see p. 20), and by the fact that disposal is unlikely to be otherwise taking place on anything like a routine and consistent basis. We were pleased to see a reference to retention schedules in an example of locally produced guidance for a weeding campaign, but note this will have limited value where correct retention criteria have not been defined. Judgments will be harder to make in the context of poorly managed or orphaned CAFs. These factors together with varying reported levels of business engagement on disposal campaigns increase the risk that HMRC is exerting insufficient control over disposal processes. It is likely to be disposing of information it should be keeping and vice versa.

In addition, we were concerned to note that Google Academy guidance, in addition to encouraging staff to move information with value from CAFs to Google Drive, states that 'Any Community, Group or Site that remains unused will be deleted by the Google Administrator'. HMRC must review this line. HMRC needs to establish a defined mandated process for disposal within the current technology environment and for management of digital information with value above the short term.

It should specifically establish a clear, central mandate for management of information with medium to long-term value is created in or moved to Google Drive. In doing so it should bear in mind that it is not yet clear whether export from Google Drive can be performed to The National Archives' required standards. **See recommendation 3**

Sensitivity review, transfer and planning

HMRC is currently not in a position to report accurate figures in the Records Transfer Report, with errors and inconsistencies evident in draft spring 2016 figures. The legacy it reports can only be a proportion of the real figure.

HMRC has no central review team. While HMRC is a digital transfer group member and attends meetings regularly, it has not begun to consider processes for the appraisal, review and transfer of digital records. HMRC is reviewing its transfer process and is not currently transferring records. **See recommendation 5**