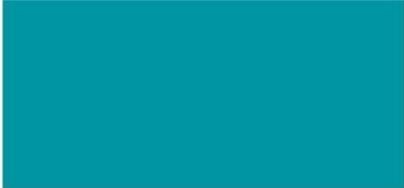


Information Management Assessment

A review of good practice from the IMA programme, 2008-16

Section 2: Information and supporting technology



Working with government to raise standards in information management



Contents

1	The technology environment	3
	Corporate storage of information	
	Finding, accessing and protecting information	
2	The continuity of digital information	10
	Encouraging joined-up planning	
	Understanding digital continuity vulnerabilities	

Note: references are to the named individuals, roles and organisations as they operated at the time of the Information Management Assessment or progress review

© Crown copyright 2016.



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

Any enquiries regarding the use and re-use of this information resource should be sent to psi@nationalarchives.gsi.gov.uk

1. The technology environment

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

Corporate storage of information

IT systems should support and enable the effective management, protection and exploitation of information. The Section 46 Code of Practice emphasises that they should be designed to meet an organisation's operational needs.¹ In relation to the creation and storage of information, it notes:

'They should be set up in a way that enables routine records management processes to take place. For example, digital systems should be able to delete specified information in accordance with agreed disposal dates and leave the rest intact.'²

In addition:

'They should be easy to understand and use so as to reduce the effort required of those who create and use the records within them. Ease of use is an important consideration when developing or selecting a system.'

Our assessments consider how IT systems have been implemented and whether they are being maintained and developed as required.³ We look for evidence that organisations are exercising adequate oversight and control over their technology environments. This includes the extent to which retention and disposal have been factored in and the action taken to limit the

¹ nationalarchives.gov.uk/information-management/manage-information/planning/records-management-code/

² Where departments have put disposal activities on hold, for example, to meet the requirements of the Independent Inquiry into Child Sex Abuse (IICSA), departments should continue to ensure that disposal capability is built into newly-procured IT systems.

³ nationalarchives.gov.uk/information-management/manage-information/ima/

ability of staff to store information outside designated shared corporate repositories.

At the time of writing, a number of departments are moving to either Microsoft Office 365 with SharePoint or a Google platform with Google Drive. We will begin assessing the success of this transition in 2017-18. The cross-government records management project is currently providing support to departments on the implementation of new records management systems to improve the management of current digital information. This is in response to recommendations made in Sir Alex Allan's 2015 *Review of Government Digital Records*.⁴ Good practice principles that are established will be built into our assessment model in the future.

Welsh Government, 2014 IMA

The Electronic Document and Records Management System (EDRMS), iShare, provided a structured environment for the lifecycle management of digital and paper information. The Welsh Government IMA report noted work undertaken to ensure that the EDRMS continued to provide an enabling environment for records management:

'Retention schedules are applied at folder level and are being actioned according to defined triggers ... Welsh Government has sought to gain further benefit from its EDRMS by standardising processes such as file creation and naming, and the allocation of privileges. This has been achieved via the "Tasks" workflow process. This effectively acts as a filter for requests from the business, supporting the consistent application of defined criteria.'

2016 progress review

At the time of the 2014 IMA there were no size limits on email accounts or automated disposal. Welsh Government also held a substantial volume of archived legacy emails. Following the IMA, Welsh Government set up an

⁴ www.gov.uk/government/publications/government-digital-records-and-archives-review-by-sir-alex-allan

improving email and records management project. The progress review noted:

‘The four strands of the project were:

- Better record management
- Improved mailbox management
- Simplified rules, guidance and support
- Standards for email behaviour

‘Aims of the record management strand included encouraging storage of all records within iShare and restricting access to alternative locations. The project recognised the need to make it easier for staff to do the right thing and included a six-month behavioural change campaign. A communications plan drove regular publication of news items and updates across a range of locations.

‘The improving email and record keeping project was established under the corporate ‘Reducing Complexity’ banner with sponsorship from the Permanent Secretary. This gave it visible senior support and placed it in the same context as wider organisational improvement work in areas including the provision of advice to ministers ...

‘To encourage storage in iShare, Welsh Government has placed a 1GB size limit on email accounts, with automated deletion of all emails after one year. It hopes to reduce this limit in the future. A limited set of exemptions were identified and temporary solutions were offered to support those with larger mailboxes or legacy information. Operations Group approval was obtained for this work and for work to tackle legacy storage in personal and shared spaces. [A] post-project evaluation] found that there had been a 64% increase in iShare usage since the introduction of mailbox limits and deletion rules.’

HM Treasury, 2015 IMA reassessment

The new SharePoint based IT system, Info Store, had been implemented rapidly. Although gaps were identified in the IMA report, we noted that the new system was an improvement on the EDRMS that was in place at the time of the previous IMA. Staff take-up was good and, crucially, the department had plans in place to address the system's limitations. We noted:

'HM Treasury has set up an Information Management Project to:

- address the digital legacy (from the first EDRM in 1996 until the move to the latest in 2013, plus orphaned data on file shares) and move it all into line with The National Archives' Gateway 1 for appraisal and selection
- redesign the SharePoint EDRM to implement better policy compliance (by design) and enable digital preservation.

'HM Treasury has recently documented requirements for the Information Management Project and the next iteration of its records management system. The Records Management Systems Requirements bring together mandatory requirements, records management requirements and business user input. They cover metadata, file plans, search, access permissions, retention and disposal, triggers for disposal and transfer to The National Archives.'

Department for Business, Innovation and Skills (BIS), 2015 progress review

At the time of its 2013 IMA, BIS faced a range of risks in relation to the availability of its information because of a lack of oversight and control exercised over its unstructured shared drives. The progress review recognised the effort that BIS had subsequently invested in preparing its shared drives ahead of the move to its new IT system:

'Seventy shared drives were rationalised onto the M drive ... Each business area had a new shared area on the M Drive, the top two

levels of which were pre-determined, and users were encouraged to move across information that they wanted ... Users are being asked to identify information that eventually will be migrated to Alfresco. The KIM team will then migrate these records across to Alfresco as it is being rolled out to business areas. Once migrated, there will be a period where the M drive becomes read only, is then hidden and then decommissioned. There will continue to be limited use of the shared drive for linked spreadsheets and access databases as these cannot be stored within Alfresco. Once shared drives have been turned off, “The Only Way is Alfresco” IT protocol, developed by the Ways of Working team, will go live and there will be a more formal switch over to Alfresco. This addresses a key concern raised at the time of the IMA around policy on the shared drives and will ensure that there is a clear line on what the shared drives should/should not be used for.’

Northern Ireland Office (NIO), 2016 IMA

Work was underway at the time of the IMA to flatten the file plan of NIO’s EDRMS, TRIM. This was expected to enable the automated application of retention criteria. We noted that take-up of the system had been better than we had seen in many other government departments with a traditional EDRMS. The IMA report stated:

[This] is probably largely due to the fact that NIO has, up to now, eliminated or controlled alternative areas for storing information. During the assessment we found a lot of positivity towards TRIM from users, despite a few issues. Staff generally find it easy to save documents and emails into TRIM. There was recognition that it is a good tool and of the benefit of keeping important corporate information in a shared space. A user from a policy area said that it was “good to be able to access historical documents” and had asked for a link in the file plan to previous work on a Bill so they could learn from these records. One or two interviewees said they disliked it at first but, once they got used to using it, they found it helpful. One interviewee compared TRIM to an

EDRM that they had used in another government department which had been difficult to search, saying that TRIM was “much easier to use”.’

Criminal Records Bureau (CRB), 2012 IMA

A specific project had been launched to address the risks relating to storage of information in personal G Drives in preference to the Corporate File Plan (CFP):

‘CRB is aware that the retention and storage of information has become an issue. Historically, CRB has not imposed a limit on the size of personal drives (G Drives). The “G Drive Project” was introduced by CRB in recognition of the fact that some staff had been using their G Drives to store information and records in preference to CFP ... The project aims to drive staff to move corporate information to the CFP by imposing a size limit of 250MB on G Drive personal storage space.

Ministry of Defence (MOD), 2011 IMA

The 2011 MOD IMA recognised the department’s efforts to address the issue of personal drive usage. In addition to the application of size limits, the assessment team noted a number of approaches including within Permanent Joint Headquarters (PJHQ) where:

‘A proactive policy of “naming and shaming” the worst offenders had been put in place to publicise the issue of records storage outside Meridio and drive people to review their personal drives.’

Finding, accessing and protecting information

Organisations should ensure that the information they create and keep is, and remains, available in line with business need. The technology environment should enable the protection of sensitive information and the appropriate exploitation of sensitive and non-sensitive information for the benefit of the

taxpayer and the business. Key requirements set out in the Section 46 Code of Practice include the ability to control access, provide an audit trail and protect records from accidental or unauthorised deletion. The Code also emphasises the fact that systems should enable quick and easy retrieval of information.

HM Treasury, 2015 IMA reassessment

Existing filing structures had been migrated into HM Treasury's new IT system, InfoStore, to help introduce an element of familiarity for staff. These were owned and maintained by business areas. Although some newly created file plans were reportedly complex, we recognised efforts at an organisational and team level to ensure effective structures were in place:

'Each business area has been asked to review and update its file plan. The KIM team has been monitoring this and will be chasing those that have not yet done this ... One business area has also introduced a "mystery shopping" approach of checks to see if its staff members could find records in other teams' filing areas. The Information Management Project will address this by assessing the structure as a whole and introducing more consistency.'

Foreign & Commonwealth Office (FCO), 2014 IMA reassessment

FCO was planning to replace its existing EDRMS, iRecords, with a new system to deliver better information and records management capability. We recognised as good practice the processes FCO had put in place within the existing system to ensure the availability and capture of one specific set of records that had been identified as having a high value, noting:

'The automated registry of Diplomatic Telegrams (DipTels) within iRecords was highlighted by a number of interviewees as a key means of ensuring the preservation and therefore the long-term availability of a high-value resource. FCO should be commended for putting this policy in place.'

2. The continuity of digital information

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

Encouraging joined-up planning

As well as providing a supportive environment for the management, protection and exploitation of current digital information, organisations need to ensure that digital continuity is maintained over time and through change. The National Archives defines digital continuity as:

‘... The ability to use digital information in the way that you need, for as long as you need. If you do not actively work to ensure digital continuity, your information can easily become unusable. Digital continuity is about making sure that your information is complete, available and therefore usable for your business needs. Your information is usable if you can:

- find it when you need it
- open it as you need it
- work with it in the way you need to
- understand what it is and what it is about
- trust that it is what it says it is.⁵

Joined-up governance for information helps support the achievement of digital continuity outcomes. Effective planning is needed to support both current business use and transfer to The National Archives where historic value is identified. Organisations should ensure that business requirements for information and records management are factored into system design from the start. We encourage organisations to ensure that digital, data and technology and KIM staff are engaging routinely and actively working to build a shared understanding.

⁵ nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/what-is-digital-continuity/

Home Office, 2015 IMA

The Departmental Records Officer (DRO) was well placed to ensure that information and records management requirements were considered during IT change and IT procurement:

‘... The DRO has good visibility of the ICT procurement process. As an assessor, the DRO has the ability to comment on and contribute to business cases. We were given verbal assurance that helpful informal links exist between IT and KIM staff. The inclusion of IT subject matter experts alongside senior business representatives as standing members of the Knowledge and Information Executive Group (KIEG) offers the opportunity to strengthen and formalise these links.’

HM Treasury, 2015 IMA reassessment

IT and KIM functions were positioned within the same business area, IWS. We saw good evidence that they were working closely together and there appeared to be a good working relationship between the two. The IMA report noted:

‘HMT was one of the earliest adopters of digital records in UK government and has not created any significant paper files since 1998. As a result, information management is seen as “digital”: there isn’t a paper and digital split of the kind we see in other government departments. Contracts and procurement are part of IWS too and have a similarly close working relationship with KIM. The KIM team has the opportunity to feed in its view as a matter of course in relation to IT procurement and contracts.’

The National Archives, 2012 progress review

We assessed our own organisation in 2011. The 2012 progress review noted improved alignment and closer relationships between IM and IT professionals:

‘The Head of KIM sits on the IT strategy panel and leads on user engagement and information management themes. KIM team membership of the Technical Governance Board has the potential to influence the development of new IT projects. It allows the opportunity for KIM concerns to be raised so that they can be addressed and factored into system and application design.’

Understanding digital continuity vulnerabilities

We assess whether organisations are working to understand what digital information they hold and identify vulnerabilities relating to its age or format. We look to see whether organisations understand the risks, particularly at times of change, and whether they are planning to ensure that digital continuity can be maintained over time.

The National Archives’ report on *the Digital Landscape in Government 2014-15* notes:

‘How digital information has been handled over time also has an impact on how records are transferred to The National Archives and on preservation once they are in the custody of The National Archives. There is also the risk that, if departments do not have good knowledge of the record formats that they hold and actively work to care for them, formats could become obsolete and departments would be unable to access their digital information, resulting in records being lost.’⁶

⁶ nationalarchives.gov.uk/documents/digital-landscape-in-government-2014-15.pdf

Department of Energy and Climate Change (DECC), 2014 progress review

The DECC IMA progress review noted the department's creation of a tailored digital continuity plan ahead of the move to its new records system:

'DECC has written an internal two-page digital continuity strategy... with a focus on the move to DECC Shares and the need to ensure that metadata and content are maintained when information is migrated between systems.'

The Ministry of Justice (MOJ), 2016 IMA reassessment

MOJ had developed its understanding of digital continuity since it was first assessed in 2010. It had put in place structures and processes to enable the management of digital continuity risks, with training and workshops provided to Information Asset Owners (IAOs). The IMA reassessment report noted:

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