The National Archives

Information Management Assessment

Department for International Development

Reviewed

November 2016

Published

October 2017

Working with government
to raise standards in information management

Contents

Statement of commitment

The following statement was provided by the Permanent Secretary of DFID. It is published on GOV.UK.

The Department for International Development last undertook an Information Management Assessment (IMA) in 2008. This was part of the regular programme of assessments that The National Archives conducts to review information, records and knowledge management standards within government departments. To demonstrate the strength of the Department for International Development's commitment, I have asked The National Archives to carry out an IMA reassessment in November 2016.

The Department for International Development recognises the importance of meeting its corporate obligations to effectively manage, protect and exploit the information it creates and holds.

The report that The National Archives produces will help me to support all aspects of knowledge and information management across the Department. It will help ensure that our information, knowledge and records are appropriately captured, managed and preserved, and information risks and sensitivities are appropriately handled.

Mark Lowcock,
Permanent Under-Secretary, Department for International Development
8 July 2016

IMA background

The Information Management Assessment (IMA) entailed a detailed review of supporting documentation followed by interviews with senior staff, specialists and practitioners in the department's London and East Kilbride offices. These were conducted between 7 and 10 November 2016. Additional interviews with key staff were conducted in person and by telephone on 24 November and 20 December.

The following report provides a summary of good practice and risks identified. 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

Key finding of the assessment

1 The value of information

Key developments since the last IMA:
• **DFID published an Information Management Strategy in 2013 which sets out its strategic priorities and maps these against the Information Principles for the UK Public Sector**

Performance rating	
Communicating and realising value	**Good practice**
Managing information as an asset	**Development needed**

- There was a good understanding amongst senior management and staff that good information management drives effective working practices. DFID would benefit from having a senior champion for information management
- DFID has developed an Information Strategy that sets the overall framework for information management. To maintain the good practice rating, this now needs updating to reflect recent changes and future direction. This should be supported by relevant policy setting out roles and responsibilities
- DFID publishes extensive information about development projects funded by the UK Government, which is good practice. Good records management is built into the standard way of working
- The Information Asset Register is not used as a tool to manage key assets, focusing instead on IT systems rather than the information held
- The IAO role could be better utilised to manage information as an asset

2 Digital information and supporting technology

Key developments since the last IMA:
• **DFID has developed and rolled out a new EDRM system, Vault, to replace Quest**

Performance rating	
Supporting information through technology	**Good practice**
Digital continuity and IT change	**Satisfactory**

- Vault should provide a solid platform for DFID to manage its information and records, provided that DFID is able to ensure that as ever-increasing volumes of information are added to Vault there is no significant drop in performance, both in the UK and overseas
- In addition to ensuring that Vault technical performance continues to support DFID's information management objectives, DFID must also work to ensure that staff receive adequate training and support to ensure they are using it effectively
- The performance issues that affected Quest resulted in some legacy risks, with some records held outside corporate systems. These risks need to be managed

3 Information risk, governance and oversight

Key developments since the last IMA:
• **DFID has adopted the Cabinet Office Security Policy Framework model of a Senior Information Risk Owner (SIRO) who is supported by Information Asset Owners (IAO) in the management of information assets which appear in the Information Asset Register (IAR)**

Performance rating	
Recognising information risk	**Development needed**
Establishing control	**Development needed**
Providing guidance	**Satisfactory**
Measuring impact	**Development needed**

- Information risk is recorded on the Strategic Risk Register but the definition focuses on the loss of information rather than wider information risk such as failure to share or exploit information
- DFID has a records management policy (Blue Book, section H3) which clearly sets out roles and responsibilities in relation to the management of records and information. This should be updated to reflect the move to Vault.
- DFID should consider how its governance structures could support better information, particularly in bringing together key information management, information assurance and information technology roles. It also needs to decide how it will monitor information and records management practice and this should be set out in the records management policy.

4 Records, review and transfer

Key developments since the last IMA:

- **DFID are now processing records through selection and transfer in line with the transition to a 20-year rule**

Performance rating	
Oversight of records and selection	**Satisfactory**
Implementing disposal decisions	**Satisfactory**

- DFID is currently managing the review and transfer process effectively and is not currently reporting any significant backlogs in its Records Transfer Report (RTR) submission
- There are a number of challenges which need to be addressed including the transition to the 20-year rule and key responsibilities sitting with one role. If DFID fails to take a proactive approach to tackling these issues, maintaining an effective review programme will be compromised.

Highlights table

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

Highlights of the 2016 IMA
DFID has an information strategy that is reviewed regularly and mapped to the Information Principles. The strategy includes specific actions to drive improved performance
DFID has developed and rolled out a new EDRM system, Vault. DFID has taken the time to consider their requirements for the new system in full and has now rolled out Vault to the entire department, including overseas offices
DFID has a real commitment to transparency and publishes large amounts of information about how its overseas programmes are run. This is commendable in itself, but also acts as a driver for good records management
DFID has developed a system of Smart Rules which set out how overseas programmes should be run. Records management aspects are included in the Smart Rules
DFID is running a project on Joined Up Search, which aims to make corporate information more findable and exploitable. Joined Up Search aims to make information held across different systems a resource for a federated search tool. If successful this would help reduce the silo effect where information is only easily available to one part of the business
There is a good working relationship between the in-house IT function and KIM, particularly in the roll out of Vault
DFID has developed good guidance on the use of online tools which states that Vault should be the only system used to store records of value

Recommendations to address risk areas

Recommendation 1
DFID should develop clear objectives for information management governance and practice within the department's new IT environment.
This would be supported by: • Updating the Information Management Strategy to include actions from The National Archives' IMA Action Plan and other strategic priorities in information and records management • A governance Board to formalise the relationship between information management, information assurance and information technology which takes ownership for the implementation of the updated strategy • Ensuring that the Blue Book is updated to reflect how DFID will monitor compliance with the policy on records management set out in section H3 • Identifying a senior champion for the new strategy and policy • Defining the role of the Information Management Unit (IMU) to guide, shape and monitor information management and records management, in line with the RM Policy • Formalising the role of the business in managing information • Ensuring that broader information management risks, such as the ability to make evidence-based decisions, are identified, assessed and mitigated as appropriate • Bringing information management related risks within scope of the information risk policy

Recommendation 2
DfID needs to gain a better understanding of the information assets it holds and the means by which these are managed, enabling effective oversight and control.
This would be supported by: • Reviewing what information is captured in the Information Asset Register (IAR) to ensure it is a useful tool to understand what information is held in order to exploit and manage the risks • Considering whether retention can be built into the IAR • Reconsidering the Information Asset Owner (IAO) role to ensure that individuals are managing risks, creating opportunities and monitoring information assets • Utilising The National Archives' training and guidance, as well as learning from other government departments such as the Department for Work and Pensions, Ministry of Justice and Northern Ireland Office • Undertaking a review to identify what records are held outside Vault, including shared drives, legacy systems and online tools • Developing a plan to manage these records, for instance by migration into Vault or utilising data analytics tools

Recommendation 3
DFID should continue its good work in implementing a system for managing digital records and ensure that good information management processes are built into Vault.
This would be supported by: • Establishing procedures to close folders in Vault to allow effective retention scheduling to take place • Undertaking a systematic review of what records are currently being held outside the corporate EDRM (Quest and Vault) and develop a plan for how records with value will be moved to Vault • Publishing DFID's retention schedules to provide greater transparency • Assessing whether records migrated into Vault – but not required for ongoing business needs – can have retention schedules actioned • Restricting individuals' ability to store information on their personal drives, possibly by reducing storage space available • Developing a system to quality assure the file structures business areas are establishing • Monitoring performance and user experience of Vault to ensure it remains effective. This should include whether staff are saving important emails to Vault • Reviewing access permissions to ensure these are appropriately applied. • Making training on Vault compulsory for all users • Implementing retention schedules for 'cold records' (see section 4.2) held in Vault

Recommendation 4
DfID needs to define how good information and records management will be championed and embedded across the business
This would be supported by: • Identifying who at a senior level should champion and drive good information management, while considering how to encourage more senior level champions • Exploring good practice in other government departments such as HM Treasury. • Arranging for The National Archives to conduct another Board level briefing to raise awareness of information risks and management • Assessing business areas' compliance with information management policy and practice. Consideration should be given to benchmarking performance and follow-up action taken against poor performance • Looking at the Digital Ninjas (see section 3.2) as an example of how to successfully drive behaviour

Recommendation 5
DfID should review what training related to information management is essential for staff to undertake, take steps to make that training mandatory and consider how it will ensure that this is enforced.

This would be supported by:

- Reviewing how new staff receive an induction into information and records management at DFID. Assessing whether the responsibility for this induction should sit with line managers or whether it should be delivered centrally
- Ensuring that all staff complete the Responsible for Information (RFI) training and that refresher training is mandated
- Develop an e-learning package for Vault which sets out clear responsibilities

Recommendation 6

DFID should develop a forward plan for the appraisal and selection of records, and their subsequent transfer to The National Archives.

This would be supported by:

- Developing selection criteria and macro approaches for appraisal and selection in order to increase efficiency and ensure processes are scalable
- Devising an approach for the appraisal and sensitivity review of digital records
- Considering the use of third party contractors to carry out cataloguing
- Clarifying the role of the Departmental Records Officer (DRO) in supporting Vault

1 The value of information

1.1 Communicating and realising value
Goal: The organisation establishes the value of information in principle and supports its realisation in practice.

Establishing the importance of information
We saw evidence of support for, and engagement with, information and records management at the highest level within DFID. The Permanent Secretary's statement of commitment on the IMA was published on GOV.UK, publicly demonstrating his commitment to the process. The Permanent Secretary also included a message about Vault in his monthly update to staff, encouraging people to 'take time to learn how to get the most out of our brilliant Vault system.'

A number of the managers we spoke to recognised the importance of good practice in information and records management, with one noting: 'DFID needs to collect the right information and manage it well to support better decisions and the right evidence base.' We also saw some evidence of commitment to good information management practice. One interviewee described the publication of information management KPIs for their office and awards given to the best performers. Another senior manager working overseas was seen as an exemplar in driving good practice in his team. When we looked at the management information provided by Vault on usage of the system it was clear that this was having a positive effect on uptake and usage of Vault across the team. DFID should continue to explore ways to engage managers to lead and champion good information management.

As it moves to embed Vault (see section 2.1), DFID has decided to adopt an approach of emphasising the individual responsibility that all staff have for their own records, rather than providing extensive administrative support. This is in line with the general culture of DFID, which was described by one interviewee as a 'self-service model'. In order for this approach to be successful DFID staff need to have a strong understanding of the value of information. While we found a broadly good culture of thinking about information and records, DFID need to ensure that staff listen to the messages being shared with them around the importance of good information and records management . It also needs to be made clear who has responsibility for championing good information management behaviours. One interviewee expressed the challenge as ensuring that DFID 'show people what works and why it matters.' See section 3 and Recommendation 4

Ensuring that staff are aware of the importance that DFID assigns to its information is an ongoing process, particularly for a department like DFID where staff move/change roles regularly. DFID should ensure that information and records management forms a core, and possibly mandatory element, of the induction of all new staff. See section 3.3 and Recommendation 5

Setting goals for information and its management
DFID has an Information Strategy 2013 which maps DFID's information priorities to

the Information Principles for the UK Public Sector and includes specific actions to drive improved performance. The Information Strategy sets out DFID's commitment to good information management, emphasising the role it plays in supporting corporate objectives, and establishes the following vision:

> Those working for DFID manage, exploit, make available and protect corporate information through systems and processes that are aligned with legislative requirements and the needs of transparency and are supported by effective policies, procedures and guidance.

The strategy was updated in 2016. DFID should now review the strategy to embed the agreed IMA Action Plan into DFID's overall strategy and ensure DFID gains full benefit from the introduction of Vault. It should also seek a senior sponsor above the level of the information management team. See Recommendation 1.

Enabling public access to information and supporting transparency and re-use
DFID receives a moderate quantity of FOI requests, approximately 100 per quarter. In Q3 2016 DFID reported having received 111 and responded to 88% of these requests within 20 working days and 100% within the permitted time (taking into account permitted extensions). DFID has a centralised FOI function. The central Information Rights team commissions information searches for FOI requests, including from lead business areas and then co-ordinates and prepares responses, ensuring they are issued promptly. During the assessment we did not find any evidence that poor records management was causing difficulties in responding to FOI enquires.

DFID publishes considerable amounts of information on the projects it runs on a website called Development Tracker. Development Tracker is built using the International Aid Transparency Initiative (IATI) standard and incorporates data from DFID, other parts of government, and DFID's delivery partners. The Smart Rules provide a guide for what records need to be published on Development Tracker. DFID's commitment to proactively publish this information is good practice in transparency.

Records published on Development Tracker are automatically exported from Quest (at the time of the assessment Quest was still used to link into Development Tracker, until the migration of records to Vault). This process supports good records management in DFID. By managing the transparency process through Quest DFID has sought to embed the behaviours and thought processes around ensuring records are held in the right place.

The Smart Rules set out how DFID will manage its programmes and defines specific information management outcomes to ensure evidence is captured of the work and outcomes of the programme (see section 3.3).

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

DFID follows the Cabinet Office Security Policy Framework model of a Senior Information Risk Owner (SIRO). The SIRO is supported by Information Asset Owners (IAOs), who are required to record information assets on an Information Asset Register (IAR). However, we saw no evidence that the model had traction within DFID. The guidance and the roles were all in place but they did not appear to be embedded in normal working practices.

The IAR has approximately 80 entries at the time of writing and assets tend to be IT systems rather than broad categories of information held within those systems. The IAR requires IAOs to record only a limited range of context that can be used to assist in the management of the assets; information such as format and the disposal policy for information in the asset is not included. Without this level of detail, the IAR is not providing sufficient oversight of the assets to allow it to be a useful tool for information management.

There was awareness among interviewees that the information asset governance was not working effectively. The process of providing assurance through IAOs and the IAR was described as being 'on pause' to allow a review to take place. DFID should review how it captures information about information assets and the reporting framework to ensure the IAR is a useful management tool. See Recommendation 2

Ownership of information assets

DFID has traditionally appointed Deputy Directors as IAOs. Guidance to IAOs sets out their responsibilities, including:

- Leading and fostering a culture that values, protects and uses information for the public good
- Knowing what information each information asset holds, what enters and leaves it, and why
- Understanding and addressing risks to each information asset, and providing assurance to the SIRO

We saw little evidence to suggest that the role of the IAO had become embedded at DFID. The IAOs that we interviewed about the role tended to view it as part of a yearly check to ensure that IT systems were being managed appropriately. In general staff did not know what the IAO role involved or who might be responsible for the information assets they worked with. DFID needs to ensure that IAOs are clear about their role and what is expected of them. DFID would benefit by exploring what other departments, including MoJ and DWP, have done in this regard, as well as making use of The National Archives and Cabinet Office training materials for IAOs. See Recommendation 2

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

DFID uses Vault – an OpenText product – as the designated corporate system for managing its digital information. Vault is a replacement for Quest (also OpenText). Vault was rolled out across the department in 2016 and Quest was used from 2005 to 2016. It was clear throughout the assessment that staff in DFID welcomed the upgrade to Vault, Quest having suffered severe performance problems in later years. Vault is a traditional EDRM and is capable of full lifecycle management, including audit trail, structure, context, metadata, access restrictions, disposal, etc. DFID's challenge now will be to balance Vault's functionality with a move to a culture of holding staff to account for their own records management and placing a suitable governance structure around this. See Recommendations 1 and 4.

In recent years DFID staff have considered it a challenge to work with Quest due to performance issues. These issues – the impacts of which were particularly pronounced in overseas offices (see below) – have resulted in staff avoiding adding records to Quest in some situations and storing them elsewhere instead. Following the introduction of Vault some people we spoke to, but not all, said that they had made a conscious effort to go back over previous work to ensure it was now added to Vault. DFID needs to identify what other repositories of records outside Quest/Vault exist and take action to ensure that there is a programme to manage these records. See Recommendation 3

The success of DFID's decision to phase out the Information Manager role and delegate responsibilities in Vault to individuals, such as setting up folder structures, in part relies on the corporate records system offering a good user experience. DFID has invested a considerable amount of time and effort in developing and rolling out Vault. The feedback relating to perception and user engagement with Vault from the people we spoke to was unanimously good. One user reported that 'Vault is fantastic and easy to use in comparison to Quest.' Another reported that Vault was quicker to use because Vault automatically pulls in metadata when you're filing, saving time.

The top four folder levels in Vault are fixed and business areas are able to tailor the folder structure under this as required. Vault is set up to allow individual users greater autonomy in setting up folders (which previously required Information Managers to action). DFID needs to establish what, if any, processes they will put in place to quality assure the structures that users will create. See Recommendation 3

As it is newly rolled-out, Vault does not contain a large amount of information at present. However, it is likely that volumes will increase significantly in the future. A requirement around ensuring that performance is not affected by the volume of

material in Vault was built into the tender process. Due to the importance of a positive user experience of Vault in DFID's KIM approach it is recommended that DFID closely monitors performance and user experience. See Recommendation 3

DFID's policy is that important emails should be filed in the corporate EDRM. Staff interviewed for the assessment were aware of this and had a good understanding that email may need to be treated as a record. DFID has a 90-day deletion policy in place for emails which is intended to ensure that staff identify important emails and take action to file them. In order to access emails beyond 90 days, staff previously had to file them in Quest. However, performance issues with Quest meant that this process could take a considerable amount of time. Interviewees highlighted a range of workarounds that they, or colleagues, had employed as a result, including saving the emails in the Calendar function of Outlook, saving them to the c: drive, and disabling the 90-day auto-delete rule.

Vault is fully integrated with Outlook and users are able to move emails into Vault through a simple, user-friendly process. The metadata that Vault requires is captured automatically when emails are filed; this should hopefully serve to reduce the use of workarounds when coupled with a programme of educating staff in how to manage their emails. However, DFID needs to ensure that it is monitoring whether staff are saving emails to Vault. See Recommendation 3

One of the key challenges that DFID faces in providing a technology platform which enables good information and records management is that much of its important work takes place overseas where the technical environment is often less robust than in the UK. For example, internet connections are often much slower, meaning access to information can be harder. This, combined with the general performance issues with Quest, has meant that staff working overseas have faced serious issues in using the system. In response to these problems staff based overseas have often saved records to their laptop hard drives or personal drives.

Records stored on non-network hard drives are particularly vulnerable as there is no ability to create back-ups of this material or ensure the digital continuity of the information. During the assessment we heard of at least one instance where a hard drive failure resulted in large quantities of records being lost. In addition to these occasional and dramatic loses of information, DFID is exposed to ongoing information risk from personal drives. Unlike records stored in shared repositories, records held on personal drives are not automatically available to others. DFID has no guarantee that such records will be shared with other staff or parts of the business, and therefore they cannot be used to support effective decision making.

We heard about staff starting to pro-actively transfer information into Vault, but DFID needs to put a corporate programme in place to ensure that records with value held on personal hard drives are moved to Vault. In addition DFID should consider what options are available to restrict users' ability to store information on personal drives in the UK and overseas. See Recommendation 3

From a technical point of view, DFID has sought to improve the performance of Vault when in use overseas by introducing a series of cache servers. Initial reaction from interviewees based overseas suggested that these measures were having a positive

impact.

The majority of shared drives were closed down when Quest was introduced to DFID; there are no shared drives in the UK. During the assessment we did learn that some overseas offices do make use of shared drives. DFID should ensure that it has oversight of any shared drives that are in use and that records are moved to Vault as required. See Recommendation 3

There are other repositories of information in DFID, for example, collaboration and productivity tools such as SharePoint Teamsites, Google Apps, Trello, and Yammer. DFID has produced a piece of guidance on what information should be held in these applications which emphasises that only Vault should be used for records of DFID business. **This is good practice**. DFID needs to monitor whether staff are following this rule and have a plan in place to address this if they are not. See Recommendation 1

Finding, accessing and protecting information
The performance issues with Quest affected users' ability to find and access information within this system. One user reported that she often noted down the unique ID reference for records that were important to her in order to find them at a later date. Another user reported that 'Unless things are filed in the right folders the search function is hard to fathom – you can get no results to thousands.'

Vault should provide users with a much more positive experience and early feedback on this is encouraging. The search function currently works well, though this may be due in part to the fact that Vault does not contain a large amount of information. It was suggested during our interviews that the effective search tool in Vault was encouraging cross team working. Interviewees had felt that previously there were silos of information because you could not find information that other teams were working on.

DFID is currently in the Discovery phase of a Joined Up Search project. The aim is to enable searching across different sources of information, both structured and unstructured. It is hoped that the project will make information much easier for staff to discover and exploit, potentially breaking down silos of knowledge. Although the project was at a very early stage at the time of interview, the ambition and collaboration across teams was commendable. DFID's KIM and IT Security teams have worked together to manage how permissions are set up within the Vault system. DFID has moved to a system where owners of folders will be responsible for managing access permissions. This will be linked to an active directory in Vault, and so, will be updated when people leave. DFID needs to carefully monitor how staff are setting up and managing access permissions, and continue to provide appropriate support and related guidance. See Recommendation 3

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
DFID's use of an EDRM system since 2005, coupled with the relative lack of a 'digital heap' of records held in shared drives, means that it has a relatively good understanding and oversight of its information held in corporate systems. The risk for DFID is that there are some sets of records where it has no oversight at all; these risks are addressed in section 2.1. DFID should work to address these gaps in its oversight. Records being held on individual laptops – outside any networked IT – are at risk of digital continuity failure. This needs to be addressed.

Vault has a number of report functions that provide management information on the use of Vault. This allows the IMU to understand with a high degree of granularity what types of information is being stored in Vault, where it is being stored, and who is using Vault.

Prior to the introduction of Quest in 2005 a print-to-paper policy was in place which required the corporate record to be held on paper. A major migration exercise was undertaken moving all digital content from shared drives into Quest. These records will need to be considered for transfer to The National Archives in line with the date the records were created. Older records are also likely to be most at risk of digital continuity failure, such as lack of support for file formats. Such records should be identified to ensure they can still be accessed and used. DFID should identify any digital information older than 2005 that was migrated into Quest to ensure there are no digital continuity risks to this information. See Recommendation 3

Digital continuity planning/IT change
DFID's IT function is in-house. This gives DFID greater control over IT change programmes. DFID's approach to rolling out O365 is a good example of this. DFID's O365 project is currently in its discovery phase. DFID is assessing whether it wants to implement OneDrive. This is good practice as it demonstrates that the business requirements are leading the decision making process.

DFID is in the process of planning the migration of records from Quest to Vault. The migration is being designed to ensure the completeness and context of the records is maintained and DFID will test the migration during the process in order to verify this. This is good practice.

3 Information risk, governance and oversight

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

Documenting and defining information risks
The DFID Risk Management Framework is underpinned by five fundamental principles: communication, documentation and evidence, professional judgement, common language for describing risk, and the application of DFID's Smart Rules. Risks are considered through six categories: context, delivery, safeguarding, operational, fiduciary, and reputational. Information risk is within the scope of this framework.

DFID's Strategic Risk Register records a risk around the 'Physical or electronic loss of sensitive information or data.' In line with this, DFID's interpretation of information risk appears broadly focussed on risks to the security of information, particularly sensitive personal information.

The impact of a records management failure may have a significant effect at a team, or even at an organisational level, if information is not available in the way that it should be. However, DFID is not currently subjecting information management related risks to scrutiny or monitoring processes to manage them through the risk management framework. At a local level, for example, it was not clear whether information management related risks were being documented by overseas offices, despite the considerable problems accessing Quest and the fact that staff were resorting to saving records on laptop hard drives.

Working to a definition of information risk which included the availability of information should have resulted in this issue being formally raised and escalated and allowed the impacts of email capture to be monitored. While DFID was aware of these problems and took steps to address them, their approach was not formally risk led. DFID must broaden their definition of information risk to include the availability of information and records and the information risk policy should include information management risks. See Recommendation 1

DFID needs to ensure that it defines the risk to the department of failing to manage information so that the impact of not capturing or keeping the information that is needed can be understood and managed at all levels of the business. The SIRO should have sight of this risk and the actions that are in place to manage it. It should also ensure that poor records management practice is recognised as a possible cause in the loss of sensitive physical or digital information. See Recommendation 2

Implementing an information risk management approach
DFID has an Information Risk Management Assessment Methodology in place in order to assess and manage information management risks in relation to the security of information. The methodology allows risks to be assessed and set out whether

SIRO level authority is required to proceed. DFID has been independently certified as compliant with ISO 27001. It works hard to ensure that IT systems are secure, for instance the IT Security team was engaged with the development of Vault throughout the process to ensure that Vault could be accredited when completed.

To promote good information management, The National Archives runs a bespoke programme of Board level briefings on Information Assurance and Cyber-Security. These awareness sessions consider strategic information risk and risk mitigation strategies. DFID's Executive Management Committee last received a board briefing in June 2014 but The National Archives would be happy to do a second briefing to help reinforce awareness of information risk and information security issues.

3.2 Establishing control

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

Governance structures
It was clear through the assessment that there were good informal communications between different information specialists working within DFID. However, there was no evidence of any strategic body that formally brought such specialists together to consider issues and share practice.

We recommend that DFID sets up a Board to integrate planning and priorities for Information Management, Information Assurance and Information Technology. The Board would also take ownership of the reviewed information strategy. See Recommendation 1

Supporting the business
The IMU provides central support for, and oversight of, KIM within DFID. It supports staff and monitors compliance, providing guidance and advice. The team has a robust plan in place that prioritises work in key areas such as auditing private office, updating guidance and managing identified digital continuity risks. In reviewing the information management policy, DFID should take the opportunity to clarify the role of the IMU to define the service it delivers to the business. This should include both how the unit supports the business through providing training and support for Vault, but also how the unit will monitor and enforce good practice. See Recommendation 1

A key priority for the IMU has been the move from Quest to Vault. This has involved the broader development of Vault by the Business Solutions Department (BSD), training and floor walking to support users, and continues post roll out through managing the process of migrating records from Quest to Vault. With the roll out complete, IMU will continue to support users of Vault through the Service Anywhere portal.

Support networks
When Quest was DFID's corporate records system a support network of Information Managers was in place to ensure the system was used appropriately. Each business

area had an Information Manager who performed a number of roles, including raising new folders in Quest, providing a first line of support and advice for Quest, and submitting a Quest Quality Assurance Return each quarter to the IMU. With the move to Vault a decision was made to discontinue the role of the Information Manager and to place responsibility for proper use of the system in the hands of the individual users. This move is in line with DFID's self-service ethos and is made possible by the increased functionality and ease of use of Vault. However, the shift in responsibility makes it particularly important that the information management related responsibilities of staff, managers and senior staff are formalised in policy as noted above. See Recommendation 1

We heard from a number of senior interviewees that one of the key challenges in good information management was changing peoples' behaviour. It is not entirely clear who owns this responsibility presently DFID. The self-service model that DFID has adopted has strengths, but potentially creates a key gap in the role of championing good information and records practice the business. The IMU will continue to promote good information and records management but DFID should consider how it will lend senior support to the team through championing good information management. See Recommendation 1

DFID runs a support group called Digital Ninjas whose role is to champion and support staff in developing digital ways of working. During the assessment we spoke to a number of Digital Ninjas to assess effectiveness. The Digital Ninja network is working well to embed 'Digital' ways of working across DFID and in considering how to develop information management champions throughout the business. DFID should look to learn lessons from the Digital Ninja role and see whether these can be applied to wider information management roles.

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

DFID's Smart Rules provide guidance about responsibilities for creating and holding records:

> The SRO must ensure that any of their programme's documents which fall into the 11 document types listed in the Transparency Smart Guide are displayed on the Development Tracker. All documents and other data for publication must be accurate, written in plain English and correctly saved to enable publication. Sensitive information must be handled appropriately and only excluded from publication as a last resort.

Embedding records management rules into the broader requirements for running programmes is good practice. DFID has a piece of guidance, 'Vault versus other tools' which communicates the importance of capturing all significant records into Vault. This is a good piece of guidance which sets out concisely what should be kept

in Vault and what other systems, such as SharePoint Team Sites, should be used for.

DFID has a records management policy which is detailed in section H3 of the blue book and sets out roles and responsibilities for the management of records and information. This should be updated in lights of the move to Vault. See Recommendation 1

What to Keep
DFID has developed retention policies to cover both Quest and Vault. DFID should consider publishing their policies on records retention in common with departments, such as Ministry of Justice. See Recommendation 3

There are gaps in retention scheduling. Capturing a record of ministerial submissions was one important area where we did encounter uncertainty about what information needs to be held as a corporate record. DFID should undertake a review to identify gaps in its retention schedules and remedy them.

Providing training
DFID's induction process should provide individuals joining the department with a solid grounding in how they are expected to manage their information and records. This is particularly important for DFID because of its new emphasis on individuals exercising responsibility in this area. The IMU used to provide an information management section for the induction process but this is no longer the case. See Recommendation 5

A number of individuals we spoke to said that DFID did not generally mandate training, or where it was mandated, there was no consequence for not doing the training. An example of this would be the Responsible for Information (RFI) e-learning course which increases awareness of information security and provides guidance to reduce information risk. During the assessment it was reported that the statistics on completion were low. DFID should consider what steps they need to take to improve take-up rates for the RFI training. DFID have identified a potential information security risk and the mitigation for that risk is available – staff undertaking the RFI training. DFID should ensure that they follow through and take steps to ensure that take-rates improve. See Recommendation 5

The roll-out programme for Vault included floor walking and drop-in sessions, and staff responded positively to this. However, training was not mandatory and only available for those who proactively sought it. DFID should consider developing a learning package to support Vault, focusing both on how to use the system and on responsibilities and behaviours. DFID should take steps to ensure that take-up of the training is appropriate, and consider making the training mandatory. See Recommendation 5

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

Measuring compliance with policy

At present, DFID does not assess or measure business units' compliance with information and records policies. The Information Manager role previously monitored usage and tried to influence poor performers. Part of the Information Manager's responsibilities was the Quarterly Assurance Report which they filed with the IMU. It was suggested during the assessment that the Quality Assurance Report, and more broadly, the Information Manager role, did not provide sufficient value to warrant the investment of time and resources.

Vault has the functionality to provide granular management information about what, and how, records are being filed into the system. This functionality could provide the basis for the IMU to provide the necessary oversight and assurance that records are being held and managed appropriately. However, we saw no evidence of any concrete plan for monitoring or for acting on identified areas of poor performance and good practice. In monitoring usage DFID will need to consider whether the IMU will also have the tools and the remit to monitor other potential repositories of records such as SharePoint Team Sites.

In developing a new approach to assessing business areas' levels of compliance with records management policy DFID should learn from how other government departments do this. The 2015 IMA of HMT identified that they have an effective benchmarking programme for business areas which measures compliance with policy and drives continuous improvement. DFID should study these examples and consider holistically how a performance framework can, support the business by providing clear responsibilities for record keeping, monitor performance against these responsibilities, determine actions to be taken when monitoring suggests performance is poor, and ensure senior staff have the information they need to understand how their teams are performing. DFID should also set out how it will monitor compliance with the records management policy in section H3 of the Blue Book. See Recommendation 1

Assessing progress against strategic goals

The 2013 DFID Information Management Strategy was re-issued in 2016 with a progress report. DFID should consider developing a process for assessing progress against its strategic goals more regularly. 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 DRO
At the time of the IMA the role of the DRO in DFID was held on an interim basis by the Principal Knowledge Co-ordinator in the Business Innovations Team. Subsequent to the assessment DFID have made the Head of the Vault development and roll out, the permanent appointment as DRO. There are challenges ahead for the review programme, as outlined below, and the DRO needs to be in a position to prioritise the review of work undertaken by the team and assess whether sufficient resources are available to carry out the work required. The change to the DRO role means that the review team is directly managed by the DRO which should support work to address these challenges.

Oversight, control and use of records
DFID has good oversight of its paper records. Paper records are stored off site at TNT. There is also limited space available at Abercrombie House where files can be stored as part of the review process. DFID has so far been able to provide accurate figures for the bi-annual RTR.

Business Units request paper files that relate to current DFID projects, this is managed through the IMU and works well.

DFID should work to ensure the same level of oversight of digital records as it currently has of paper.

Appraisal and selection
At present appraisal and selection is carried out principally by one experienced reviewer with some support from other members of the IMU, where available. DFID is currently managing the process of determining what records need to be selected for permanent preservation well. It consistently reports very low (single figure) numbers of legacy records in the Information Management Report which suggests that it has an effective process for appraisal and transfer in place. The National Archives considers DFID's appraisal work to be of a high quality. DFID are currently reviewing their 1988 to 1991 paper registered file series which will need to be appraised and transferred to The National Archives by the end of 2017. DFID also have paper records going up to 2005 which will need to be processed by the end of 2025.

There are however a number of issues which DFID will need to address in order for the IMU to continue review and transfer effectively. The transition to a 20-year rule means there is a considerable amount of business as usual review work to process and the review team may struggle to keep pace with this requirement if and when

other ad hoc work is required, for example, in relation to inquiries such as The Independent Inquiry into Child Sexual Abuse (IICSA) and the Iraq Inquiry. Knowledge and expertise of appraisal and selection is concentrated in one individual and there is a risk that DFID will not be able to continue to meet its statutory obligations under the Public Records Act should this person decide to move on from the role.

In addition, appraisal and selection is currently being carried out at the file-by-file level with the considerable but tacit knowledge of the reviewer being used to interpret each record and determine its historical value. This produces good results but is time-consuming. In the past there has been some exploration of whether DFID could move to review records at a prefix level, but it was felt that the contents of each prefix were too broad to make decisions at that level. The current process is not set up to be easily scalable, nor are the skills and knowledge it relies on easily transferable.

A knowledge transfer process should be developed, including documenting selection criteria, to allow the current review approach to continue in the event of a change of personnel. DFID should also consider developing a more macro approach to appraisal and using Series Level Appraisal Questionnaires. It should engage with its Information Management Consultant (IMC), who will be able to provide further advice and put the department in touch with other government departments who have adopted this approach. This will help to ensure that DFID has the right processes in place to review the remaining 15 years of paper records. See Recommendation 6

DFID also needs to develop an approach to appraisal and selection of digital records. The National Archives does not anticipate that file-by-file review will be sustainable for digital information. The consideration of digital methods of appraisal should therefore dove-tail with the reassessment of paper appraisal recommended above. Again, the IMC will be able to support and advise DFID in this work. DFID should also sign up for The National Archives' digital transfer training. See Recommendation 6

4.2 Implementing disposal decisions

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

Triggers for disposal

Vault assigns business classifications to each folder and each of these have disposal schedules. Disposal will not be activated yet due to the restrictions imposed by IICSA. A limited amount of disposal took place in Quest; DFID implemented a retrospective exercise in 2013 and 2014 to map retention periods to Quest folders – this exercise was completed shortly before the restrictions imposed by IICSA came into force.

In order to effectively implement retention scheduling in Vault, business areas will need to close folders and DFID needs to ensure that the right personnel and

processes are in place to make this happen. See Recommendation 1

The migration of records from Quest to Vault will divide the records into 'hot' and 'cold' collections. The 'hot' records are those that have been identified as having ongoing or immediate business value and will be migrated into the Vault folder structure. The 'cold' records will not be migrated into the main Vault folder structure but will be held in a separate 'Quest Library.' Subject to the constraints imposed by IICSA, DFID should consider plans to implement the retention schedules for the cold material in order to test process and procedures ahead of implementing routine retention scheduling in Vault. See Recommendation 3

Sensitivity review

The IMU reviewer carries out sensitivity review of paper files. This means that the sensitivity review process is facing the same challenges as the appraisal and selection work, with DFID's knowledge and expertise in this area held predominately by one individual.

The records that DFID is currently sensitivity reviewing date from the period prior to 1997 when DFID was the Overseas Development Administration, a part of the FCO. As such, DFID works closely with FCO on the sensitivity review of their records. FCO is the subject matter expert on application of the s27 FOI exemption (international relations) which is one of the main areas of sensitivity for DFID records. The close coordination that is required with FCO does cause some issues, in that DFID is reviewing files relating to subjects and events at different times to FCO, but DFID is currently managing these issues effectively.

DFID has not yet started to develop an approach for the sensitivity review of digital information and needs to acquire the skills to deal with this. DFID should draw on the work that The National Archives and other government departments are doing on digital sensitivity review, particularly around tools to assist the process, and should start to plan and develop an approach. A good starting point would be the research report on *The application of technology-assisted review to born-digital records transfer, Inquiries and beyond* published by The National Archives.

DFID's commitment to transparency and the proactive publication of considerable amounts of information about development projects is commendable and should make the process of sensitivity review simpler over time.

Transfer and planning

DFID is currently keeping pace with the transition to the 20-year rule. DFID registered files work in 3-yearly cycles and the 1988-1991 files are currently being processed. The 1988-1991 file-cycle will need to be processed by the end of 2017 and DFID need to be aware of the challenges already outlined in the selection process and ensure that they continue to be compliant with the Public Records Act. DFID has a plan in place to review up to the 1995-1997 cycle.

TNT currently prepares DFID files for transfer. Cataloguing work is done by the IMU reviewer. DFID has considered the possibility of using a third party contractor to carry out cataloguing and decided that good catalogue descriptions required a level

of knowledge and experience of DFID that was not available through a third party. However, given the range of challenges facing the review and transfer programme there are benefits in re-investigating this.

DFID needs to develop an approach for the transfer of its digital information (see section 4.1). DFID has previously attended meetings of the Digital Transfer User Group and should continue to engage with, and learn from, The National Archives and other government departments' experience.