

Information Management Assessment

Criminal Records Bureau

March 2012

About Information Management Assessments

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

IMA reports highlight areas of best practice and make recommendations for improvements. These recommendations will form the basis of an action plan against which progress will be tracked.

For more information about the programme and to view previous reports and action plans, see nationalarchives.gov.uk/information-management/our-services/ima.htm

About the Criminal Records Bureau (CRB)

The CRB is an Executive Agency of the Home Office. Under the Protection of Freedoms Bill, CRB is due to merge with the Independent Safeguarding Authority (ISA) to become the Disclosure and Barring Service NDPB in 2012.

For information about CRB, please visit <http://www.homeoffice.gov.uk/agencies-public-bodies/crb/about-crb/>

Table of Contents

1	RISK MATRIX	4
2	KEY FINDINGS OF THE ASSESSMENT	5
3	SUMMARY OF RECOMMENDED ACTIONS	9
4	SUMMARY OF GOOD PRACTICE	13
5	HIGHLIGHTS AND AREAS FOR IMPROVEMENT	15
	APPENDIX ONE: GLOSSARY	36
	APPENDIX TWO: THE ASSESSMENT TEAM	38

1 Risk Matrix

Indicative score drawn from the pre-assessment analysis, on-site interviews and evidence submitted:

Governance and leadership		Compliance	
Strategic management		Staff responsibilities and delegations	
Business objectives		Policies and guidance	
Management controls		Training	
Resourcing		Change management	
Risk management			
Information and records management		Culture	
Creation		Commitment	
Storage		Staff understanding	
Appraisal, disposal and transfer		Knowledge management	
Management of information			
Digital continuity			
Access to information			
FOI/Data Protection			
Re-use			
Security			

Key to colour coding	
Best Practice	
Good	
Satisfactory	
Development needed	
Priority attention area	

2 Key findings of the assessment

- 2.1 The Criminal Records Bureau has a focused, operational remit which is to process around 4 million disclosures per year. There are many examples of good practice in the organisation, particularly regarding risk management. This puts CRB in a sound position ahead of the proposed merger with the Independent Safeguarding Authority (ISA) to become the Disclosure and Barring Service (DBS). This is expected to complete in 2012. The project to oversee this is named 'One Organisation'.
- 2.2 CRB is focused on information security and data protection, however risks relating to the inability of CRB to use its information are not actively managed. The agency has excellent networks throughout the organisation supporting information assurance and records management, effective and high profile staff in key Information Management (IM) roles, and a committed senior leadership team with a history of delivering change on core priorities. As a result, CRB is in a position to respond quickly and embed further good practice. This gives the agency the capability to drive real improvements in IM prior to change and shape effective working practices in the new organisation.
- 2.3 This report highlights the areas of good practice that should as far as possible be embedded within the new organisation. The report also highlights **8 recommendations** for improvement that will support CRB to manage and assure its information ahead of the merger and the move to a proposed Electronic Document Records Management System (EDRMS) solution.

Governance and leadership

- 2.4 The Agency has a close relationship with the Home Office and the new Agency Record Officer network. CRB currently operates under the Home Office IM strategy. This provides consistency of process and policy across the Home Office group. However CRB needs to develop its own IM plan to sit underneath the Home Office strategy if it is to ensure the effective management of information over change.
- 2.5 CRB has an active and engaged senior management team, and IM is

supported by an effective Business Integrity Unit (BIU), where staff have developed a high profile and positive reputation throughout CRB. This has allowed CRB to drive important and meaningful change, exemplified by the effective delegation of responsibility for ownership and management of information assets to the Information Asset Owners (IAOs). IAOs have visibility in their teams, feel able to perform their responsibilities, can escalate issues when required and feel supported by the IAO network. **This is good practice** and CRB should continue to roll out this model for Records Advisors (RAs).

- 2.6 CRB is aware of and manages those risks related to information security and the Data Protection Act, proactively seeking external assurance in these areas. CRB is now beginning to take action to address wider information risks that have been identified, such as the 'G Drive Project' which seeks to address the storage of information on personal rather than corporate repositories. These are encouraging but need to be fully embedded.

Information and records management

- 2.7 Retention within the Customer Relationship Management (CRM) system is not actively managed and information is not deleted. CRB needs to evaluate the risk, benefit and cost of disposing of personal information that is no longer required in the CRM system, with a view to deleting this prior to the anticipated merger with ISA.
- 2.8 In the other major records system - the Corporate File Plan (CFP) – retention is implemented inconsistently and staff do not always store records and information in the correct place. This puts the capture of records at risk and may affect the ability of CRB to function effectively and account for decisions that have been made. CRB needs to raise the level of staff understanding to ensure that they know what to keep, where and for how long. It needs to be recognised in particular that email is part of the corporate record.
- 2.9 CRB has begun proactively to address some of these issues via the 'G Drive

Project' and the inclusion of retention on the Information Asset Register (IAR).¹ In an important project, BIU are working with Records Advisors (RAs) in business units to create bespoke retention schedules for CRB business areas. **These initiatives and projects are important and represent a good start.** However they need further senior support and local monitoring if they are to be fully embedded.

Management of digital information

2.10 The vast majority of CRB's work is digital. CRB needs to build on the work already done to identify and record assets, and define the way in which it needs to use the information that it is creating. This will ensure that CRB can manage its information effectively over the 'One Organisation' change and the anticipated move to a new EDRM system.

Access to information

2.11 The Information Commissioner's Office (ICO) Data Protection audit gave CRB a rating of 'high assurance'. This demonstrates robust risk management processes.

2.12 CRB makes publication schemes available via the CRB section of the Home Office website. In September 2011 the CRB executive team agreed to expand the range of information it proactively publishes and increase the amount that is published in a re-usable format.

2.13 At the time of the assessment, CRB's Freedom of Information (Fol) response rate for 2011 was 100% (including extensions). The implementation of a 'What to Keep' project and a focus on increasing staff understanding of records will ensure that CRB does not lose its current level of performance.

2.14 Security is proactively considered at CRB and is factored in to the creation of systems. Security sweeps are conducted to ensure that information security is

¹ Since the assessment, Business Criticality and Business Purpose have also been included as headings on the IAR.

being managed effectively and its importance recognised at a senior level.

Compliance

2.15 Despite its prominence in training and guidance, the Government Protective Marking Scheme (GPMS) is not well understood throughout CRB and rarely is applied correctly. Training must be provided to CRB and Capita staff and compliance needs to be monitored.

2.16 CRB has a range of guidance available to help staff to understand their responsibilities. Much of this is directly taken, or derived from, Home Office guidance. CRB has recognised the need for tailored retention guidance and is working with business units to develop this. **This is good practice.**

Culture

2.17 Senior management recognise the importance of getting the buy-in of middle management to drive future changes. This group is recognised as crucial in delivering long term benefits as part of the 'G Drive Project'.

2.18 Staff understanding about security and information assurance is generally good. However, staff understanding about wider information management risks and issues needs to be improved if CRB is to demonstrate best practice. For example, staff were aware of the 'G Drive Project' but the majority could not articulate its purpose, despite significant efforts to raise awareness. A lack of middle management buy-in and monitoring has affected the take up and buy-in to the aims, limiting the impact and efficacy of the project.

2.19 There is no overall strategy for knowledge management in CRB. However, there are a number of positive examples such as the sharing of knowledge and experiences about risk management at the Risk Improvement Forum (RIF) and IAOs talking about their information assets at quarterly meetings. **This is good practice.**

3 Summary of recommended actions

These recommendations will form the basis of an action plan that will be monitored.

Ref.	Summary recommendation	Paragraph:
1	<p>Develop a CRB specific information management plan.</p> <p>The plan, which will sit under the Home Office IM strategy, will define how CRB needs to manage its information up to and through the proposed merger, as well as the move to the new EDRM system. As this will include business process and technology change, CRB needs to:</p> <ul style="list-style-type: none">• Ensure that success criteria are defined in advance.• Ensure that digital information is effectively managed over the proposed merger.• Ensure that digital continuity requirements are incorporated into the development of any new technology solution and are considered as part of any migration exercise.²• Ensure that adherence to the plan is monitored at board-level.	5.4, 5.30
2	<p>Expand the scope of the Information Asset Register (IAR) to create a tool to support information management.</p>	5.7, 5.14,

² Guidance on embedding digital continuity in your IM practices is available from nationalarchives.gov.uk/documents/information-management/embedding-dc-in-info-management.pdf. For guidance about incorporating digital continuity in change management and your IT environment and supporting tools such as a migration checklist, see nationalarchives.gov.uk/information-management/our-services/digital-continuity-stage-4.htm.

	<p>The upcoming business process and technology change increases the urgency of this action. The IAR should be used to inform planning for any changes to CRB's technical infrastructure and as a means of testing the usability of digital information after change. As a minimum action, CRB should include at least the following fields:³</p> <ul style="list-style-type: none"> • Requirements to be able to find, access, work with, understand and trust digital information.⁴ • Users of the information (including sharing requirements). • Technical dependencies. 	5.28, 5.30
3	<p>Develop Key Performance Indicators (KPIs) to monitor use of Corporate File Plan (CFP) and monitor these at board level.</p> <ul style="list-style-type: none"> • This should ensure that managers within teams are promoting, monitoring and enforcing the goals of the IM plan, 'G Drive Project' and retention. • Develop KPIs to monitor use of CFP. This should ensure that managers within teams are promoting, monitoring and enforcing the goals of the IM strategy, and 'G Drive Project'. 	5.19, 5.20, 5.22, 5.34, 5.40, 5.45, 5.49
4	<p>Evaluate the risk, benefit and cost of disposing of personal information that is no longer required in the Customer Relationship Management system (CRMS), with a view to deleting this prior to the anticipated merger with ISA.</p> <ul style="list-style-type: none"> • CRB needs to make a decision based on an assessment of the risk, cost and benefit. Weeding prior to change is likely to make it cheaper at time of re-contracting. It also means less information to manage over change and less complex data migration. 	5.21

³ Since the assessment, Business Criticality and Business Purpose have also been included as headings on the IAR.

⁴ Guidance is available from nationalarchives.gov.uk/information-management/our-services/digital-continuity-stage-2.htm

5	<p>Implement a coherent programme of training and a review of guidance available to raise the information management capabilities of staff.</p> <ul style="list-style-type: none"> • Update the mandatory introduction training to include the section 46 principles covering records management. This needs to include an explanation of what constitutes a record (including email), what staff need to keep, where and for how long. • Incorporate the updated 'What to Keep' schedules into training and guidance when completed. • Identify and satisfy the need for training in the application of GPMS. • Evaluate means to increase take-up and awareness of available guidance. 	<p>5.20, 5.22, 5.34, 5.43, 5.47, 5.50</p>
6	<p>Evaluate the possibility of mandating against the use of pst files for storage of emails.</p> <p>The use of pst files puts the ability of others to find and access information at risk. CRB needs to evaluate the viability of mandating alternative working practices and ensure that email records are stored in an appropriate system.</p> <ul style="list-style-type: none"> • Assess the risks and benefits of by June 2012 	<p>5.25</p>
7	<p>Evaluate and assess how best to utilise RAs to promote and monitor information management good practice.</p> <p>RAs need to be enabled to perform their function through access to training, time and resources:</p> <ul style="list-style-type: none"> • Continue the development of the RA Network • Senior management need to ensure that line managers and departmental heads understand the importance of the RA role to CRB and allocate sufficient time and resources to allow them to effectively discharge their duties. 	<p>5.20, 5.40, 5.41, 5.45, 5.51</p>

	<p>RA responsibilities need to include:</p> <ul style="list-style-type: none"> • Supporting managers to monitor CFP usage and progress of the 'G Drive Project'. • Applying retention according to the bespoke retention schedules being developed • Disseminating best practice guidance and promoting IM policies and procedures within their teams 	
8	<p>Ensure that information is managed appropriately over the merger.</p> <p>CRB needs to:</p> <ul style="list-style-type: none"> • Set up an Information Transition team, to assure the information that the organisation relies on is being managed through technology and business change⁵ • Define roles and responsibilities for developing requirements and managing information over change • Ensure that testing after change ensures that information remains complete and available. 	5.27

⁵ For advice regarding the management of change, please see nationalarchives.gov.uk/documents/information-management/dissolution-of-public-bodies.pdf. The National Archives has also produced guidance to support the change of status. This is available at nationalarchives.gov.uk/information-management/projects-and-work/reform-public-bodies.htm. A checklist is available for migration of digital information between systems at nationalarchives.gov.uk/documents/information-management/edrm-migration-checklist.pdf.

4 Summary of good practice

The following have been specifically identified as examples of good practice in this report.

1	<p>The SIRO has effectively delegated responsibility for management of risk to Information Asset Owners (IAOs) through the creation of an engaged network with support structures. Over 30 IAOs have been appointed at SEO grade and above. They have quarterly meetings with the SIRO, complete quarterly returns, update the Information Asset Register (IAR) and are assigned administrators. Quarterly meetings actively engage individuals, with IAOs talking about their information assets and sharing best practice. IAO's reported feeling supported by the structure and IAO network, and the provision of administrative support demonstrates the recognition by CRB about the importance of the role. CRB should continue to roll out this model for RAs.</p>
2	<p>CRB has recognised the need for tailored retention guidance and is working with business units to develop it. This will support the application of retention within teams, and should be used to raise awareness amongst staff of the value of records and information to CRB.</p>
3	<p>CRB has recognised the need to identify information assets held within business areas and record these on the IAR. This has increased CRB's oversight and ability to manage information and have been safely able to dispose of information assets that are no longer required.</p>
4	<p>The 'G Drive Project' is a positive initiative that was set in motion after a potential issue was identified with the</p>

	amount of information being stored in personal drives. The project aims to reduce the amount of digital information and records held on personal drives in order to ensure CRB is well prepared for the anticipated move to EDRMS. This needs to be further embedded within the organisation.
5	The Risk Improvement Forum is a forum for the open discussion of the types of risk and possible mitigations. This seeks to share knowledge and experiences in an informal way. Interviewees who had attended recognised the important role of the forum in sharing best practice and recognised the value to the business.
6	The Senior Leadership Forum is an initiative that enables issues to be flagged and support to be gained for policy initiatives and strategic priorities among senior managers.
7	CRB has in place robust and collaborative processes for managing Data Protection risks. This is reflected in the rating of <i>high assurance</i> given to CRB in a recent DPA audit conducted by the Information Commissioner's Office.
8	CRB will expand the information it publishes proactively and seek to make it available in re-usable formats where possible . This includes reviewing and publishing procurement and contract information, details about the board structure, IARs (previously only available on request) and frequently requested statistical information.

5 Highlights and areas for improvement

Governance and leadership

Strategic management

- 5.1 The Criminal Records Bureau (CRB) is an executive agency of the Home Office, with which it maintains a close relationship. This is a pragmatic decision with the benefit of providing support and networks for CRB, including an Agency Records Officer network and bi-monthly security meetings. Home Office also provides a policy framework under which CRB operates, with CRB adapting and producing tailored guidance as necessary. This increases the likelihood of compatible ways of working when systems (such as the HR and Finance system Adelphi) are shared.
- 5.2 CRB is in a period of transition, with a merger and change of status scheduled to take place in 2012/13. The agency is expected to merge with the Independent Safeguarding Authority (ISA) to become the Disclosure and Barring Service (DBS),⁶ a Non-Departmental Public Body (NDPB). The merger (known as the 'One Organisation' project) requires re-contracting for ICT, scanning and post-room services. CRB will also be brought on to the Home Office EDRM system in Q3/4 2012. This will replace the current corporate records management system, Corporate File Plan (CFP), which is also hosted and administered by Home Office suppliers Fujitsu.
- 5.3 Positively, CRB has recognised the need to understand its business processes ahead of the merger. The Business Plan 2011/2012 states the need for a 'clear, well-constructed plan for the move to becoming one organisation'. This

⁶ At the time of compiling this report (January 2012), this is dependent on the Protection of Freedoms Bill 2010-11. Subject to parliamentary progress, the bill is expected to receive Royal Assent by the end of the current session.

is to be developed in conjunction with ISA and Home Office. The Service Transition Project in CRB is working alongside representatives from business areas to assess what functions the business units within CRB perform. It is defining distinct 'work packages' that will inform the tender for the new system and the exercise will also be used to consider the necessity and value of functions.

- 5.4 CRB does not have a tailored information management strategy in place, choosing instead to work to the Home Office IM Strategy. The assessment team acknowledges that there are many tangible benefits to this approach. CRB needs to develop a specific information management plan to ensure it is effectively managing its information risk and requirements, particularly over the merger process. This needs to sit under the Home Office strategy and ensure that the impact of technology and business change do not adversely affect the ability of CRB to use its information. **See recommendation 1.**

The information landscape

- 5.5 CRB's expected merger and planned move to Home Office EDRM system increases the importance and urgency for the agency to define its information requirements.
- 5.6 CRB has begun to make progress to understand the information that it creates, stores and uses. There has been a drive to identify information assets held within business areas and record these on the IAR, alongside retention requirements. CRB has increased oversight and ability to manage information and has been safely able to dispose of information assets that are no longer required. **This is good practice.**
- 5.7 CRB needs to expand on this by documenting the usability requirements of its information assets prior to any migration of digital information. This will enable senior management to be confident that the impact of change on the

information is being managed and exposure to risk is minimised. **See recommendation 2.**

Business objectives

- 5.8 CRB benefits from a strong and visible senior leadership. There are clear routes for the escalation of issues. The dynamism of the executive team is clear and they are recognised as being central to driving change.
- 5.9 The Business Plan for 2011/12 recognises that the 'lawful and appropriate treatment of personal data is essential for our successful operation and helps to maintain confidence between the CRB and the data subjects and organisations with whom we conduct our business.' This obligation to manage personal data has been given prominence by the Executive team and SIRO and this is reflected in the structures that exist to manage risk.
- 5.10 The majority of the work that CRB does relates to the processing of disclosures. This is predominantly done through the CRM system. The Executive team and senior management have put in place robust and collaborative processes for managing associated DPA risks, seeking external assurance of their processes and compliance and ensuring escalation and early monitoring of issues within Capita post room and scanning. This is reflected in the rating given to CRB in a recent audit conducted by ICO. **This is good practice.**

Risk management

- 5.11 Information risk is mainly considered in terms of security and information assurance. Some mature and robust risk management processes are in place, with a strong IAO network and delegated responsibility. Business risk registers capture the risk for CRB and Capita, and CRB is compliant with IAMM level 3.

Risk is monitored on Business Risk Registers and boards. The RIF, a forum for the open discussion of risk and mitigations, is a good initiative and **an example of good practice**.

5.12 CRB has a comprehensive Corporate Risk Management Strategy and the structures in place to manage Data Protection and IA risks are effective. In recognition of this, CRB was the subject of a Best Practice Management case study in July 2010 ⁷ The assessment team found some evidence that CRB is starting to consider wider information risk. For example, the risk of not being able to find and make use of corporate information is acknowledged by the 'G Drive Project'. This has been introduced to address the use of personal drives for storage of records and is **an example of good practice**.

5.13 The SIRO has effectively empowered IAOs with a sense of ownership and responsibility, with effective support networks created. Over 30 IAOs have been appointed at SEO grade and above. They have quarterly meetings with the SIRO, complete quarterly returns, update the Information Asset Register (IAR) and are assigned administrators. Meetings were described as proactive and are actively aimed at driving engagement, with IAOs delivering individual presentations and sharing best practice. IAO's reported feeling supported by the structure and IAO network, and the provision of administrative support demonstrates the recognition by CRB about the importance of the role. **This is good practice**.

5.14 The IAR is used to support the management of information assets, and the recent inclusion of retention has supported CRB to delete information assets that are no longer required. **This is good practice**. Ahead of the merger, CRB needs to broaden the scope of the IAR to include risks to the information asset. Since the assessment, *criticality* has been introduced as a heading on the IAR. CRB needs to ensure that the full spectrum of information risks are considered, and that staff are aware of the value of information to the organisation. CRB

⁷ *Management of Risk within the Criminal Records Bureau*, July 2010, The Stationary Office Ltd.

should expand their IAR to include the risks that the business will be exposed to if the ability to find, access, work with, understand and trust its information is lost. **See recommendation 2.**

Information and records management

Management of information

5.15 CRB uses 3 primary systems; CRM, CFP and Adelphi (for HR and Finance).

The majority of CRB's business process depends of the CRM system, which stores and processes requests for disclosures. CFP is used to store all other information, including that relating to investigations. It is an NTFS-style system administered by Home Office delivery partners with a controlled file plan.

5.16 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 Drive). 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 assessment team heard that this was due in part to the perception that CFP is time consuming and complex to use. 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.

5.17 CRB relies on staff to distinguish between documents within the CFP that are work in progress and documents that have become records and should be transferred to a separate records area. CRB policy states that after a year documents should become records or be deleted if no longer required.

5.18 The assessment team heard examples of good practice, where the CFP is organised by date and the RA removes folders that are due for deletion each December, in line with a standard retention schedule. However, the majority of staff did not understand the distinction, or the purpose, of separating documents and records. Some staff reported not having enough time to sort through their information to move documents in to records, elsewhere the practice was inconsistent and ad hoc. Some staff also expressed concern that moving documents to the records area creates 'uncertainty regarding having two places to look' for records.

5.19 The aim of the 'G Drive Project' is to support the proposed transition to a new EDRM system by ensuring that corporate information is appropriately saved on the CFP and can then be migrated. This has delivered benefits in areas with high value records such as Private Office which had not previously been distinguishing between documents and records. Middle managers are key to success and need to drive change within their teams, lead by example and ensure monitoring and compliance. Key Performance Indicators (KPIs) should be developed to monitor use of CFP (including retention) and reported at board level. **See recommendation 3.**

5.20 The inconsistency found by the assessment team means that CRB cannot yet be confident that information and records in the 'Documents' have been consistently moved across to 'Records'. After the completion of the 'G Drive Project', it is important that RAs continue to provide best practice support and advice, training and continued monitoring of CFP use. **See recommendations 3, 5 and 7.**

What to Keep

5.21 Whilst the CRM system has been given high assurance by the ICO, it remains the case that there is no retention applied to core records. Personal information relating to approximately 26 million Disclosure applications is retained on the CRM system. This contravenes Principle 5 of the DPA and exposes the organisation to operational and reputational risks. Senior management are aware of the risks and need to decide about whether to delete the records according to existing retention policy, or as part of the new ICT contract. Guidance produced by The National Archives recommends that prior to business or technology change, ephemeral information, or information that is no longer required by the organisation or parent department 'should be

securely disposed of according to approved retention policies'.⁸ Reducing the volume of information is also likely to bring down the cost of re-contracting and reduce the complexity of managing key assets. CRB needs to determine its own risk appetite before assessing the cost, benefit and risk associated with each option. **See recommendation 4.**

5.22 CRB currently uses generic Home Office retention schedules which are not tailored to the records and information CRB creates. A retention project has been set up to work with RAs and IAOs to define and document the retention in individual business areas. **This is good practice.** CRB needs to continue the project embedding within business units and monitor compliance. **See recommendations 3 and 5.**

Appraisal, disposal and transfer

5.23 Because of their age and status, CRB has not transferred records directly to The National Archives. CRB, together with Home Office and The National Archives⁹, needs to consider the capture of records that may be of interest to the future record (such as board minutes) and how this will be managed after the change of status. This should be embedded in the bespoke retention schedules.

Email

5.24 The management of emails appears to be inconsistent. Whilst the 'CFP User Guide and Information Management Handbook' outline the roles and responsibilities for saving email, interviewees did not consistently understand

⁸ See nationalarchives.gov.uk/documents/information-management/dissolution-of-public-bodies.pdf. Also see Cabinet Office guidance <http://umbr4.cabinetoffice.gov.uk/media/332838/mog-handbook.pdf>. The Home Office IM Strategy also cites the case study of Serious Organised Crime Agency, concluding that it is 'better to clean records in the old system than the new system'.

⁹ See The National Archives *Guidance on the Management of Private Office Papers* nationalarchives.gov.uk/documents/information-management/popapersguidance2009.pdf.

them to be part of the corporate record. It is not explicitly part of the RA role to manage email inboxes or ensure that retention is being applied. There is a risk that information is not shared appropriately or is lost.

5.25 Staff are also widely using pst folders to archive emails. This has contributed to the volume of information held within G Drives. Information stored in inboxes and pst files may not be obvious when seeking to answer Fol queries, may be lost when staff depart and may also be stored longer than needed, raising risks to CRB under the Data Protection Act (DPA). CRB needs to mandate against the use of pst files. **See recommendation 6.**

Management of digital information

Digital continuity risk¹⁰

5.26 CRB will be undergoing a series of changes within the next two years. Initially the impact on the disclosure of records is expected to be minimal. However, 'One Organisation' will entail an as yet unspecified complex technology change and may include business process change, as CRB expands its remit to provide basic checks and issues certificates directly to the applicant.

5.27 The changes may also involve the loss of specialist knowledge and compromise between CRB's requirements and those of ISA and DBS. CRB needs to develop a digital continuity plan, as part of the IM plan. This must take into account the need for CRB to define its usability requirements for its information, how to deliver these and technical dependencies.¹¹ CRB needs to manage the risks to their information over this process¹² and ensure that records management considerations are built in to any new technology system, including any successor to CRM. This must include, but not limited to, retention. **See recommendation 8.**

5.28 CRB has made a good start with their Information Asset Register, which now includes retention. Expanding the IAR further would allow CRB to create a management tool that can document the agency's requirements. As a minimum requirement this should include Business Risk, Risk to the Asset and

¹⁰ Digital continuity is the ability to use your digital information in the way that you need, for as long as you need. See nationalarchives.gov.uk/information-management/our-services/dc-what-is.htm.

¹¹ For guidance, see nationalarchives.gov.uk/information-management/our-services/digital-continuity-stage-2.htm.

¹² When contracting, CRB will need to ensure that the ability to find, access, work with, understand and trust its information is reflected in service procurement and contracts. See *Digital Continuity in ICT Services Procurement and Contract Management* nationalarchives.gov.uk/documents/information-management/digital-continuity-in-ict-procurement.pdf. For information about managing digital continuity through technical change, see nationalarchives.gov.uk/information-management/our-services/digital-continuity-stage-4.htm.

requirements to find, access, work with, understand and trust.¹³ Doing this will enable CRB to make informed, risk-based decisions about the impact of change on their records and information management and provide further support when testing information after change. **See recommendation 2.**

Technical change management

5.29 CRB has a representative on the Programme Board which is implementing a new EDRM system across the Home Office family. Whilst there are advantages to the standardisation of systems across Home Office and its agencies, CRB requirements had not formed part of the development of the EDRM. It was not within the scope of this assessment to provide a qualitative assessment of the records management capability of the new EDRM.

5.30 Business requirements were taken into consideration when evaluating the suitability of the EDRM solution. However, as far as possible, CRB also needs to assess its suitability against the requirement to be able to find, access, work with, understand and trust its information assets. This will support CRB to make informed decisions about the suitability of any system to support information management, for example the ability to import, export and control access, as well as identify and manage any associated risks to its information. **See recommendations 1 and 2.**

¹³ See the digital continuity IAR template at nationalarchives.gov.uk/documents/information-management/iar_template.xls

Access to information

Data Protection Act (DPA)

5.31 The CRB 2011/12 business plan states that the agency adheres to the 'DPA principles of Information management, which require the treatment of information as a corporate asset, improving the quality and value of our information, thus preventing unauthorised disclosure and destruction.' Senior management recognise the importance of managing personal information, and its importance to the agency's reputation. CRB were recent subjects of a consensual Data Protection audit by ICO, which gave them an overall score of *high assurance*¹⁴, having considered Data Protection governance, training and awareness, records management and security of personal data. This is reassuring, and demonstrates a proactive approach. This report will not duplicate the findings of the ICO audit.

Re-use and transparency

5.32 CRB meets the requirements of the Transparency Agenda, making its publication scheme available via the CRB section of the Home Office website. This is managed by the FOI team. CRB have sought to do more to make information publicly available. In September 2011 the Executive team agreed to publish proactively some procurement and contract information, details about the board structure, Information Asset Registers (previously only available on request). Currently, the majority of information published by CRB is published in pdf or Microsoft Word format. There has also been agreement on the publication of frequently requested statistical information, and to increase the amount of information that is published in a re-usable format. **This is good practice.**

¹⁴ Of the four categories of assurance considered by the ICO, *high assurance* is the highest, followed by *reasonable*, *limited* and *very limited*.

Freedom of Information (Fol)

- 5.33 Up to the end of August 2011 CRB received 63 direct Fol requests and the response rate at the time of audit was 100% (including extensions). This is very encouraging. CRB state that it also receives approximately 15 'cross-cutters' (those that request information from the whole of the Home Office group) per month. Statistics are kept manually by the central team and the process of retrieving the information is the duty of the responsible business area.
- 5.34 Information kept in personal areas and inadequate record keeping practice in some parts of the business may inhibit the ability of CRB to respond effectively to Fol requests and identify all the information required. CRB needs to continue to ensure that the correct exemptions are being applied and that these are recorded and accessible. Initiatives to improve management of information and records, such as a successful 'G Drive Project', and monitoring and application of retention will positively impact on the ability of CRB to continue to maintain 100% compliance with Fol, as it supports the ability to find, access and trust information. **See recommendations 3 and 5.**

Security

- 5.35 The Assessment team were informed that historically some interviewees' access rights and permissions on CRM have been increased but not revoked when no longer needed. CRB assured the assessment team that this issue had been identified and action had been taken to mitigate the risk following an internal audit recommendation. Lessons learned from this should be used to inform CRB's technical requirements for any successor CRM system.
- 5.36 Compliance with the Information Assurance Maturity Model (IAMM) is taken very seriously within CRB. Currently the organisation is compliant with level 3. It is aiming for full compliance by the end of 2011 and level 4 by 2012.
- 5.37 There is a strong emphasis on driving compliance with security policy. Breach

processes have been introduced in relation to clear desk policy. Internal Audit has also been asked to conduct an assessment of security compliance. Induction training prominently includes security. Senior interviewees recognised the importance of communications and raising awareness as a means of driving compliance and improvement.

5.38 Downloading information from the CRM is controlled by software and an algorithm is also used to target spot checks on staff access to historic records stored in the system. Staff appeared aware of these measurements and the importance of access records on the basis of need.

Compliance

Staff responsibilities and delegations

5.39 RAs have an important role in administering, monitoring and policing CFP. The role involves acting as a gateway between the user and Home Office CFP delivery partners, arranging the ad hoc creation of folders, application of permissions as well as naming folders. On a weekly basis, RAs are expected to monitor 10% of the electronic documents in their areas of CFP to ensure compliance with IM policy and retention. Monthly duties include undertaking floor walking, giving advice about records management, and monitoring disposal dates. Clear guidance and a useful booklet is made available to the RAs outlining their responsibilities. The role is reflected as an objective in their personal development review (PDR). However, a significant number of RAs interviewed expressed concern over the amount of time needed to discharge their responsibilities properly. Whilst CRB are developing a support network for RAs based on the successful IAO network (this is good practice and one meeting had been held at the time of the assessment), the assessment team found that the role is not always given the highest priority as it is performed in addition to other duties.

5.40 The RAs also have an important role to play in the monitoring and application of retention; however, time and understanding of the business did not always allow this. One RA described moving whole document folders across to the records area in one go, without weeding or regard to what was of long-term interest. Some RAs were also concerned that they could not implement retention effectively and delete ephemeral information because of a lack of time and in-depth understanding of business processes. CRB should continue to create clearly defined, bespoke retention policy for each business area and monitor its application. This will support RAs to apply retention at a local level.
See recommendations 7 and 3.

5.41 RAs should be used to monitor compliance with policies and initiatives (such as use of CFP, compliance with 'G Drive Project'), apply retention in-line with the bespoke retention schedules (when completed) and to disseminate guidance and best practice advice to the team. In order for RAs to monitor and drive positive changes they need to be afforded sufficient time and resource in their business areas. This will require the understanding and commitment of line managers and heads of business units. CRB should evaluate the current RA role with a view to ensuring that they are focusing on the priorities of driving good practice, retention and monitoring compliance. **See recommendation 7.**

5.42 IAOs appear clear about their objectives and confident in their roles. All of those interviewed felt supported by CRB and the IAO Network. This has empowered the users and puts CRB in a good position to manage its information over the upcoming changes. Staff reported readily approaching IAOs about new assets, and the delegated responsibility appears to be working very well.

Government Protective Marking Scheme (GPMS)

5.43 Staff did not appear confident in the correct application of GPMS. Monitoring takes place but this is focused on identifying those people sending protectively marked information where they should not have, rather than those not applying protective marking. Some staff stated that they rarely saw protectively marked material, and there was also some concern expressed by interviewees that some staff are routinely overprotecting information. Correct implementation of protective marking will support CRB to ensure that its information is being effectively protected and shared appropriately. CRB needs to provide refresher training and consider other methods to raise awareness and compliance, such as guidance. CRB needs to ensure that this is also reflected by Capita. **See recommendation 5.**

Policies and guidance

5.44 CRB relies heavily on Home Office policies and guidance. These are often tailored in to CRB specific guidance. For senior management, this homogeneity supports the close working with Home Office, which facilitated the sharing of systems such as the move on to the Adelphi Finance and HR system.

5.45 CRB have produced a range of guidance for staff. The 'Information Management Handbook' explains basics such as Data Protection Act Principles, FoI and the role of the ICO. It details the obligations staff have to manage data under the acts and suggests best practice regarding the naming and storing of information, such as rules to follow when naming documents. This is a positive initiative. Staff have a good understanding about the need to protect personal data, however the assessment team found that understanding of other responsibilities highlighted in the handbook remained low. This includes section 46 and the need to store and manage records. A programme of championing information management by RAs (**see recommendation 7**) and line managers and enforcement of compliance with the introduction of KPIs (**see recommendation 3**) will support this.

Training

5.46 New RAs are provided with the guidance and associated guidance materials via hyperlink. Ad-hoc training is provided by the DPO or experienced RAs. The majority felt that they had enough support to help them perform their tasks. As one RA described: 'we were a little bit in the dark, but now we have plenty of support'.

5.47 CRB is facing a large number of changes. Consideration should be given to training and induction provision and the needs of the organisation to learn new skills – especially with the changes to the new EDRM system and 'One Organisation'. The National Archives' guidance to support section 46 states that: 'All staff, including temporary staff, contractors and others working for the

organisation, should receive induction training that outlines the organisation's records management policies, standards, procedures and guidelines and makes clear their personal responsibilities.¹⁵ CRB needs to embed section 46 records management advice into their training. Whilst it is mentioned in the induction training and 'Information Management Handbook', it does not have a high visibility and staff remain uncertain about what constitutes a record. A programme of training is required to ensure staff are confident about what to keep, what to destroy, where to store information, how and why retention is applied. **See recommendation 5.**

¹⁵ nationalarchives.gov.uk/documents/information-management/rm-code-guide2.pdf

Culture

Staff understanding and commitment

5.48 Staff understanding of security and information assurance is generally good.

This comes as a result of a concerted effort, driven by the board and supported by governance structures and networks. However, CRB needs to raise staff understanding about the wider information management risks and issues. The assessment team found that the majority of staff had heard about the 'G Drive Project' and the need to reduce personal drive sizes, although only a small minority could articulate what the purpose and benefits are. This is despite a number of communications being issued to staff and team brief articles which are cascaded from line managers. The DPO also reiterated the message through Data Protection Reviews. However only a small number of interviewees reported that their line manager had reiterated this message or monitored compliance within their area. The assessment team noted examples of staff who had stored corporate information on personal drives, rather than CFP, which had caused problems when others had needed access to the information.

5.49 There is commitment from senior management to improve information management capability throughout CRB. Networks exist to support staff with their roles and responsibilities, and there are examples of senior management driving change. Senior leadership needs to ensure that there is real buy in to their aims at business unit management level, to sustain changes. At present, positive initiatives have visibility throughout the organisation, but not all have achieved buy-in. KPIs and targets for managers to ensure monitoring and embed ownership would support this. **See recommendation 3.**

5.50 CRB recognises that the introduction of new systems will require a change in culture. Plans are in place for pilots, training, guidance and monitoring of the new EDRM system, when it is introduced. This is proactive but in order to get

the most out of the training, this needs to go hand in hand with **recommendation 5**, to ensure staff understand their general IM responsibilities, not just how to use particular systems.

Knowledge management/transfer

5.51 The Senior Leadership Forum is an initiative that enables issues to be flagged and support to be gained for policy initiatives and strategic priorities among senior managers. **This is good practice** and is an effective channel to drive change in CRB. The Senior Leadership Forum should support the 'G Drive Project' and recommendations to support and reinforce the RA role. **See recommendation 7.**

5.52 A number of staff noted that CRM was useful tool for detailing the contact that an individual had with CRB, which means that if someone gets in touch with them, it is easy to see what stage their application is at and who to pass them on to. This supports efficient working and customer service, and will support CRB to meet its aims of providing a 'consistently high level of service ... in terms of accuracy and speed [and maintaining] high levels of customer service'.¹⁶

5.53 Some IAOs are asked to speak about the information assets they are responsible for at quarterly meetings. **This is good practice** and an example of good knowledge management, as awareness of risks and issues are shared.

5.54 The merger of CRB presents issues of staff churn and loss of knowledge, making it even more important that knowledge and requirements are captured. This is particularly important at this early stage, as changes will not all happen at once and may occur some time after the initial merger. There is some evidence of knowledge capture when staff leave. CRB have a knowledge

¹⁶ See www.homeoffice.gov.uk/publications/agencies-public-bodies/CRB/crb-corporate-publications/crb-business-plan-11-12?view=Binary

transfer checklist for when staff leave or change position. CRB should ensure that current procedures and consider how to capture the knowledge of SCS staff prior to the merger. Good knowledge management relies on staff knowing what information and expertise is available – and how to access and exploit this. CRB is making good progress identifying the information that it holds. The project to identify information assets has increased the awareness within teams and among senior management of what information is created, used and stored by CRB.

5.55 The Risk Improvement Forum (RIF) is a positive knowledge-sharing initiative and **an example of good practice**. This shares information about risk and risk management in an informal way. Interviewees who had attended recognised the important role of the forum in sharing best practice and recognised the value to the business.

Appendix one: Glossary

BIU	Business Integrity Unit
CFP	Corporate File Plan
CRM	Customer Relationship Management system
DBS	Disclosure and Barring Service
DPA	Data Protection Act
DROID	Digital Record Object Identification, a file profiling tool developed by The National Archives
EDRMS	Electronic Document Records Management System
FOI	Freedom of Information
GPMS	Government Protective Marking Scheme
IA	Information Assurance
IAO	Information Asset Owner
ICO	Information Commissioner's Office
IM	Information Management
IMA	Information Management Assessment
ISA	Independent Safeguarding Authority
IT	Information Technology
KIM	Knowledge and Information Management
KPI	Key Performance Indicator

NDPB	Non-Departmental Public Body
RA	Records Advisor
RIF	Risk Improvement Forum
Section 46	Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000
SIRO	Senior Information Risk Owner
SRO	Senior Responsible Owner
WTK	'What to Keep'

Appendix two: The assessment team

The assessment was conducted by members of the Standards Department and specialist colleagues from The National Archives on 8th – 10th November 2011.

The assessment team comprised:

- Standards and Information Policy Manager
- Head of Standards
- Standards Advisor
- Information Management Consultant

Assistance provided by CRB:

The Assessment team are grateful for the cooperation and assistance of all staff at CRB who were interviewed, provided additional information or facilitated the assessment process.

Our particular thanks are extended to Elaine Carlyle and Suzanne Held for their organisation and hospitality.