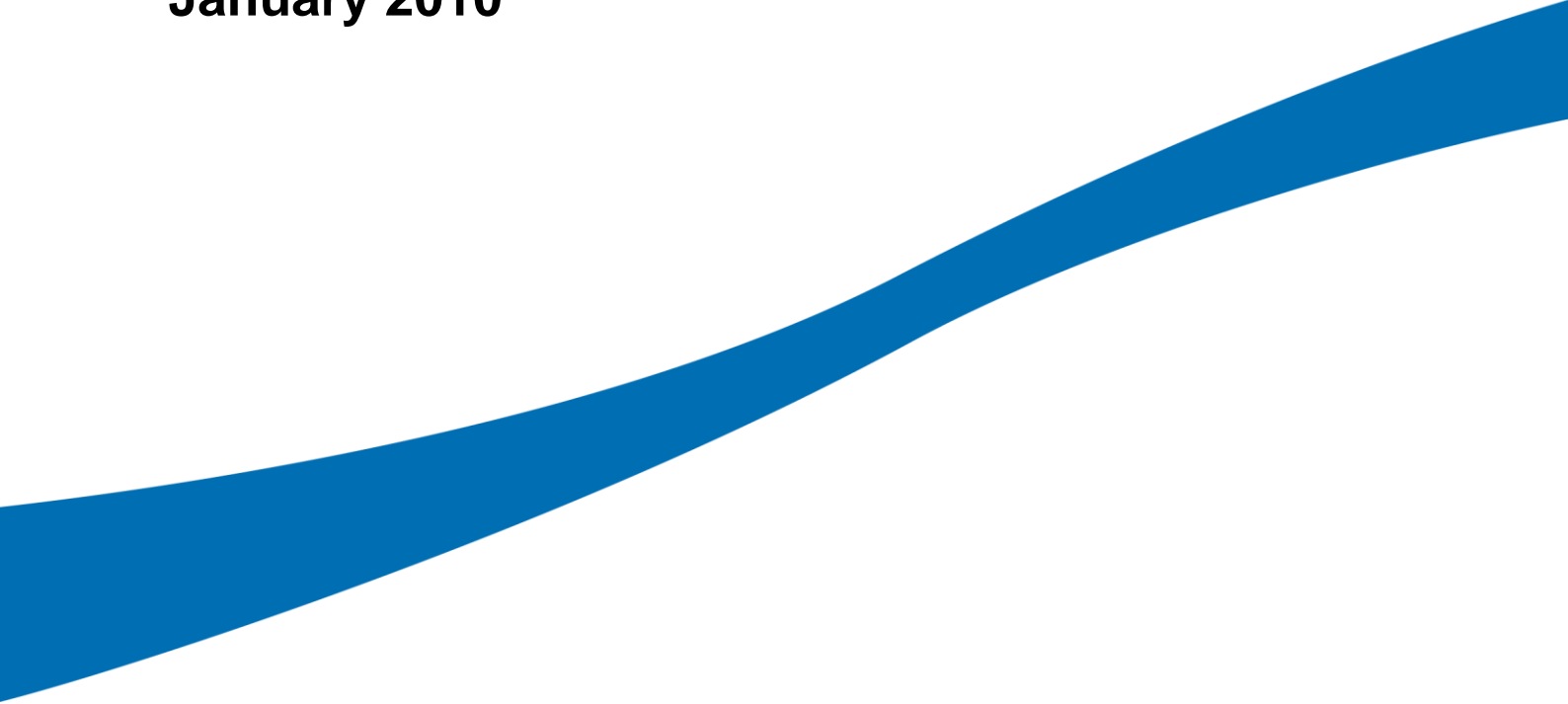




**CabinetOffice**

# Protecting Information in Government

**January 2010**



# Contents

	Introduction from the Cabinet Secretary	3
	Foreword from the Information Commissioner	5
1	Context	6
	Use of information and technology has transformed public services	6
	Emerging risks to information	6
2	Improving Information Risk Management: The Data Handling Review	8
	Promoting a culture that values and protects information	8
	Improving the procedures for managing information risk	13
	Ensuring the right technology is available to protect information	18
	The wider public sector	19
3	Looking to the Future	22
	Sustaining the change	22
	Coordination	23
	Long-term risks	25
	Conclusion	25
	Annex A	27

The Data Handling Review was published in June 2008, putting in place a set of mandatory measures for government on protecting personal data. The report committed government to report annually on the progress made in meeting the requirements of the review, and work on information risk that will be necessary in the future. This is the first such report.

## Introduction from the Cabinet Secretary

Smarter, more efficient and convenient public services depend on the right information being available, reliable, and well protected. It is therefore a necessity that we make sure that the risks to this information are properly managed.

In June 2008, we released the first report into cross government data handling procedures. That report put in place a set of unprecedented mandatory measures for government departments to improve the way in which government manages and handles personal data. This report takes stock of the progress made since the publication of the Data Handling Review<sup>1</sup> (DHR).

Government departments have been, and continue to be, firmly focused on improving their ability to protect and handle personal data. A great deal of hard work has been done and much achieved in this period. As with any form of risk, there can never be guarantees that every risk to information can be avoided; as the DHR made clear, managing risks to information will always be an ongoing task.

Changing data handling culture remains the greatest challenge – not just for government, but for every sector. In the past it had become too easy to think that a tiny memory stick was not something that needed to be particularly protected. But when it contains names, dates of birth, financial details and other important and personal information then its value increases significantly; changing a seemingly minor and replaceable piece of technology into a very valuable commodity which must be treated accordingly. The ease and speed with which we can now move significant amounts of data around should not obscure just how important that data is for the individual who has entrusted it to government.

We have made significant and far-reaching progress in bringing about a culture change in the way that we value and handle personal data. We have tightened processes and enhanced the skills of public sector staff that handle personal data with well over 450,000 civil servants trained in data security awareness since the publication of the DHR.

The new requirements have helped achieve a level of unparalleled transparency and scrutiny. Strict monitoring and compliance regimes mean that losses and near misses are more reliably reported allowing the lessons to be learnt, and help make sure that they do not happen again.

Accountability has been strengthened with responsibility for managing departments' information risk firmly established at Board level. In addition, there are now over 9,000 Information Asset Owners (IAOs) in government with responsibility for how information is handled at a business level. These are not new appointments but information security is now a core part of their existing roles.

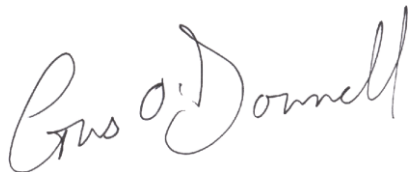
Of course, technical precautions are equally important. Government departments have encrypted laptops and other mobile devices which hold personal data. As theft of mobile

---

<sup>1</sup> <http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/dhr/dhr080625.pdf>

devices is always a threat, these measures provide an important layer of security when all else fails.

The overwhelming majority of the data handled by the government is handled properly and securely. It is an essential part of many public servants jobs. Millions of record transfers and transactions are safely conducted enabling effective and efficient public services to be delivered every day. And while we continue to do more with less to meet the challenges of the economic downturn, including bringing greater efficiencies and savings, the task of improving information security will always be a continuing process with no room for complacency.

A handwritten signature in black ink that reads "Gus O'Donnell". The signature is written in a cursive, flowing style.

**Sir Gus O'Donnell, Cabinet Secretary**

## **Foreword from the Information Commissioner**

I welcome this report, and the progress made over the last 18 months in ensuring the secure use of personal data in government. It marks an important step in bringing greater openness and transparency to the ways in which government handles our personal data.

All organisations should inspire public trust by collecting and using personal information fairly, responsibly and securely. Sustaining and building upon the measures put in place by government to improve the handling of information will significantly reduce the likelihood of incidents and problems in the future.

It is clear that there remains no room for complacency. As organisations continue to use information, and do so in new ways, government must keep pace and ensure that the right protections are in place to safeguard public trust.

Armed with our new powers of assessment, the Information Commissioner's Office (ICO) will aim to help Departments to live up to their commitments. In this way, the ICO will be helping to keep Whitehall up to scratch. But we also have a major job of education to do, helping organisations, both public and private, stick to the rules and keep out of trouble.

A handwritten signature in black ink, appearing to read 'Christopher Graham'.

**Christopher Graham, Information Commissioner**

# 1 Context

## **Use of information and technology has transformed public services**

1.1 The increasing use of information across society, in all sectors of the UK, and other countries has transformed the way that people conduct business and interact with each other. Government is no exception to this trend and a host of new technologies and business models and new ways of using information have been employed to deliver better, more convenient and efficient public services. For example:

- 18 million people are enrolled in the Government Gateway<sup>2</sup>, safely accessing 164 public services available online. These range from giving employers ways for to advertise jobs, to members of the public seeking state pension forecasts.
- NHS, social care providers and voluntary organisations have worked to enable many more patients to choose to be cared for at home if that is their preference. This requires the use of information to give a better understanding of the people receiving a service, their preferences and decisions.
- More than one million job searches take place a day using the Jobpoint service available in job centres, libraries and supermarkets across the country using up to the minute information on job vacancies across Europe.
- More efficient use of information also allows government to provide better value for money. For example, sharing back office operations and IT will play an important part in securing the £35 billion of savings<sup>3</sup> targeted over the period of the 2007 comprehensive spending review.

1.2 There are also cases where sharing information is crucial. For example, in order to protect national security, prevent crime, or support the protection of the public.

1.3 Public services are increasingly no longer provided by single departments. Departments collaborate with each other, with local authorities, the NHS, charities and with commercial organisations in order to deliver efficient and effective personalised services. These approaches bring improvements to services and savings to the public purse. They also mean that more effort and investment must be made in protecting the information used, and enabling these changes.

## **Emerging risks to information**

1.4 These changes clearly deliver great benefits for government and for the public, but they also bring new challenges. Managing risks around sharing information can sometimes become complicated when more than one organisation is involved. Equally challenging is the fact that data can be stored on very small devices such as memory sticks which, if lost, can put information at risk in greater quantities than before.

---

<sup>2</sup> [www.gateway.gov.uk](http://www.gateway.gov.uk)

<sup>3</sup> [http://www.hm-treasury.gov.uk/d/oep\\_final\\_report\\_210409\\_pu728.pdf](http://www.hm-treasury.gov.uk/d/oep_final_report_210409_pu728.pdf)

- 1.5 The continuing pace of technological change, the prevalence of social networking, the growth of mobile means of accessing the Internet and the advent of Web 2.0, and Web 3.0, mean that the ways in which information is used will continue to pose challenges to how we protect information that is held or transferred.
- 1.6 As information becomes an ever greater part of how we live our lives, it inevitably becomes a more attractive target for those who might seek to exploit that information for their own purposes. E-crime, cyber attack and other threats have risen in tandem with the overall growth of the Internet. In addition, as the devices we use to store information become more portable they become an easier target for opportunistic criminals.
- 1.7 As we go forward, we need to continue to look to find ways of delivering services which meet the needs of the modern citizen whilst taking proportionate and measured steps to manage the risk of deliberate or negligent action which might lead to the compromise of personal information.



## 2 Improving Information Risk Management: The Data Handling Review

- 2.1 The Data Handling Review (DHR) identified the areas where government needed to improve its data handling capability and put in place a firm set of rules for departments to follow. Though there will always be more to be done to manage any kind of risk, this section looks at the progress made by government in addressing cultural change, information risk management and technical precautions. An assessment of progress in implementing the DHR milestones can be found in Annex A.
- 2.2 The changes in the way that government manages information risk can be divided into three categories:
- Promoting a culture that values and protects information
  - Improving the procedures for managing information risk through measures such as accountability and external scrutiny
  - Ensuring the right technology is available to protect information

### **Promoting a culture that values and protects information**

- 2.3 Organisational culture is one of the most powerful ways in which information risks can be managed because it affects, and reflects, the way that people think and the way that they behave. This means that the right culture can mitigate many different kinds of risk in many different situations. Government has taken steps to ensure that the value of information is understood, HR procedures are bolstered, and that the regulator's powers are strengthened to help bring about the right kind of culture across the Civil Service.

#### *Understanding the value of information*

- 2.4 Hundreds of thousands of civil servants handle information of different kinds, on paper and on computers, every day. It is essential in doing so that they recognise the value this information has; both to the individuals concerned, and to the organisation that needs to use it to deliver services. This means that government must aim to have staff at every level that value information as an asset, protect it appropriately and share it securely.
- 2.5 Government has made significant progress since the publication of the DHR in raising awareness of the value of information. According to the results from a pilot of the Civil Service people survey<sup>4</sup>, 93% of staff in the organisations that participated are aware of data security policies and put them into practice.

---

<sup>4</sup> The pilot survey included 11 public sector organisations. The full people survey will be published later in 2010. More information can be found at <http://www.civilservice.gov.uk/news/2009/october/staffsurvey.aspx>

2.6 Other evidence<sup>5</sup> suggests that around 40% of private sector organisations provide ongoing security awareness training for their staff.

### Case Study 2.1: Organisational culture in government

Considerable effort has been invested across government in evolving a working culture that supports the proper handling of information. This work, like initiatives such as Health and Safety, will take time to mature but significant progress has been made by Departments.

HM Revenue & Customs has undergone an extensive programme of cultural change; training all 90,000 staff; running a series of training events with nationwide coverage, providing clear policy guidelines, and developing new ways of communicating data security messages to staff.

**Data security is your personal responsibility**

Data Security Programme  
Governance and Security

HM Revenue & Customs

**HM Revenue & Customs**

## Data Security - Golden Rules

Please remember

- Data security is your personal responsibility. Know the rules for handling the data in your care. Stick to those rules rigidly.
- Before making data available to anyone else, you must make certain you have the authority, including the legal power, to release it.

- Never access data unless it is part of your job and you have a business need to do so.
- Never give out any data over the phone or in any other way unless you are absolutely sure who you are giving it to and that they are entitled to that data.

**In the office**

- Never leave data out on your desk when you are not around.
- Always 'lock' your computer when leaving your desk.
- Choose your password carefully and never let anyone else know it.
- Challenge anybody you see in your building who is not wearing an appropriate security pass.

**On the move**

- Never take data out of the office unless you really need to. Keep your laptop, BlackBerry and any official papers secure at all times. Never leave them in an unattended car overnight.
- When working outside, you must make sure you are not overheard and that data cannot be seen by others.

**Sending data**

- Always make sure you know what protective marking the data should have and stick to the rules for that level of protection.
- Be certain you are sending only what you absolutely need to send and no more.

2.7 Training and awareness programmes are one important way in which government can influence and foster cultural change. The Cabinet Office, in conjunction with the National School of Government (NSG) has produced an e-learning package, 'Protecting Information' which has been shortlisted for 5 e-learning awards<sup>6</sup>. Some departments have developed bespoke training for their staff and in total, more than 450,000 staff across government have now successfully completed enhanced training on protecting information. Training and awareness programmes will continue in future years in order to ensure that further progress is made in promoting a culture that values and protects information.

<sup>5</sup> [http://pwc.co.uk/pdf/BERR\\_2008\\_Executive\\_summary.pdf](http://pwc.co.uk/pdf/BERR_2008_Executive_summary.pdf)

<sup>6</sup> [www.elearningage.co.uk/awards.aspx](http://www.elearningage.co.uk/awards.aspx), [www.ittrainingawards.co.uk](http://www.ittrainingawards.co.uk), [www.e-governmentawards.co.uk](http://www.e-governmentawards.co.uk)

- 2.8 To help drive cultural change through all elements of service delivery government has also made the e-learning package available to its contractors and delivery partners.

### Case Study 2.2: Mandatory training for those who handle personal data

Protecting Information presents staff with some of the situations and choices they may face in handling and using information safely in the working day. The training package provided by Cabinet Office is available, free of charge, to all public service organisations.

**Information**  
use it - don't lose it | Protecting information: Level 1

EXIT x

CabinetOffice National School of Government

Protecting Information: Level 1 / Why do we need to protect information?

**Respecting the information of others**

Most of us do everything we can to protect our personal information and can feel quite concerned when things go wrong. To gain a clearer understanding of why we should handle every sensitive piece of information with the utmost care, let's consider a scenario that will be familiar to all of us - payday.

**Image 1: Payroll slip**  
We assume that on the day we are paid, we'll receive the correct wages, on time and in the right account. We rely on other people for this to occur.  
Providing others with your personal information and bank details involves a degree of trust.

**Image 2: Computer monitor with 'Keep it secure' text**  
You expect your payroll department to keep your details safe and secure. What might the consequences be of this information going missing or falling into the wrong hands? At the very least, you might not get paid on time, or even worse - you might have your account hijacked and emptied.

**Image 3: PIN pad**  
As this demonstrates, many of the everyday processes that we take for granted require the use, sharing and protection of information. Whenever you use information, remember that it belongs to a person or an organisation. Protect information as if it were your own. Click **Next** to continue.

The e-learning training has now been accessed by over 500 organisations in central government, wider public sector and supplier organisations.

- 2.9 A further, more advanced, training module has been produced to meet the needs of those with specific information handling responsibilities, such as Information Asset Owners (IAOs) and line managers. This training is also relevant to roles that focus on policy, project management and procurement. Feedback and the monitoring of uptake and performance are helping inform the development of further training.

### Case Study 2.3: Organisational culture in government

The Ministry of Defence (MoD) has targeted a large group of public servants many of whom are not desk based (e.g. security guards, messengers, technicians, receptionists and thousands of service personnel and warehousemen). However they all handle information and need to do so securely. MoD has developed an awareness package for this group tailoring the IA message to be relevant and meaningful to their working environment.

## It could happen to you



We assume that on the day we are paid, we'll receive the correct wages, on time and into the right account. We rely on other people to do this.

Providing others with your personal information and bank details involves a degree of trust.

You expect your payroll department to keep your details safe and secure.

What might happen if this information goes missing or falls into the wrong hands? You might not get paid on time, or even worse – you might have your identity stolen and your account hijacked and emptied.

Whenever you use information, remember that it belongs to a person or an organisation.

**Protect information as if it were your own.**

- 2.10 In order to provide the right support to senior managers across government, the Cabinet Office and CESG<sup>7</sup> have also provided extensive training and workshops to support staff carrying out specific IA roles, e.g. Senior Information Risk Owners (SIROs) on a monthly basis since the inception of the Data Handling Review. This training sets out the individual's key responsibilities and puts them in the wider business context. In this way common issues and best practice are identified and shared. Information risk training has also been provided to departmental audit committees through a series of regular seminars run by the National School of Government and HM Treasury. In addition, the 2008 Best Practice in Audit Committee Conference focused entirely on information risk.

<sup>7</sup> CESG is the National Technical Authority for information assurance and a key partner in the improvement of information risk in the UK

### **Case Study 2.4: Organisational culture in government**

Culture change messages are most effective when couched in the context of the environment where change is required. Several departments have responded by producing IA training and awareness materials specially suited to their working culture.

- The Department for International Development's training DVD 'Security Matters' provides relevant scenarios which then prompt discussions on the best way to deal with the types of information security risks that staff may experience working overseas.
- The Department for Transport has placed considerable emphasis on training and supporting its IAOs. They hold quarterly seminars allowing IAOs to share good practice and learn from each others' experiences. The department has devised specific training that all IAOs must complete before they take on the role. This ensures that IAOs are fully aware of their responsibilities and know how to assess and manage the risks to the information assets under their control.
- The Home Office has developed and delivered a series of Risk Management Workshops for all IAOs to encourage collaboration and knowledge sharing within this community. The workshops also provide hands-on training for IAOs, help with the capture of information assets, and provide consistency in the management of information risks across the Home Office.
- The Foreign and Commonwealth Office employs staff locally at embassies around the world. All staff are now aware of information handling procedures. FCO has translated IA training and guidance into various languages to ensure all staff understand the potential risks and proper processes.
- HMRC have produced a short, pocket-sized, reference booklet clearly summarising the rules and how to seek advice on data handling.
- The Department for Work and Pensions (DWP) have instituted a wide, pervasive and effective data security programme with an award winning communications campaign to all staff helping to make the protection of information something everyone thinks and cares about.
- The Ministry of Justice's Communications Strategy delivers its message through a range of media including corporate and agency intranets, foyer displays, corporate bulletins, newsletters and magazine articles, 'lunch and learn' sessions and a literature series.

2.11 Government organisations are now working to complement baseline training with further, targeted work aimed at driving cultural change. For example, The Centre for the Protection of National Infrastructure<sup>8</sup> has developed and piloted a security culture review and evaluation tool which provides insight into an organisations current and desired security culture. This allows organisations to understand their strengths, weaknesses and identify areas where improvement would facilitate cultural change. The tool is being made more widely available across government, and will help support the drive to change organisational security culture. It will

---

<sup>8</sup> <http://www.cpni.gov.uk/>

ensure that information security matters are brought into the context of overall departmental security concerns.

#### *Strengthening HR procedures*

- 2.12 In addition to the efforts made to ensure that information is properly valued it is also important to focus on the public's legal right to expect that their information will only be used in the public interest, be properly handled by government, and that their privacy will be protected.
- 2.13 Government departments have amended HR processes where necessary to enforce that failing to apply the appropriate controls can amount to gross misconduct. These measures help make sure there is a clear understanding of the consequences for failing to comply with the policy put in place, and the importance of safeguarding information.

#### *Strengthening the regulator's powers*

- 2.14 The Information Commissioner's Office (ICO)<sup>9</sup> is the UK's independent authority set up to uphold information rights in the public interest; promoting openness by public bodies and data privacy for individuals. Following the DHR the ICO now has the power to conduct spot-checks on government departments without prior notice. The Government has recently formalised this arrangement by including provisions in the Coroners and Justice Act 2009 to introduce assessment notices (spot-checks) into statute. The Government has now laid Statutory Instruments providing the ICO with the power to impose civil monetary penalties on data controllers who deliberately or recklessly breach the data protection principles.
- 2.15 In addition, the Ministry of Justice has undertaken a consultation to commence the provisions in the Criminal Justice and Immigration Act 2008 that increase the penalties for breaching the Data Protection Act (DPA), as set out in section 55, to a maximum of a two year custodial sentence<sup>10</sup>.

#### **Improving the procedures for managing information risk**

- 2.16 The management of risk is, and will remain, an important part of the way that Government and other organisations deliver on their aims. There are well established procedures within organisations intended to address risk. The DHR strengthened these measures and updated guidance and policy accordingly. This has been achieved in three ways:
- Improving planning;
  - Establishing clear governance and accountability; and,
  - Enhancing the tools for managing information risk

#### Improving planning

- 2.17 Many information risks can be managed or avoided by early identification, allowing robust plans and mitigations to be put in place. This should take place in the early stages of project and policy planning.

---

<sup>9</sup> For more information on the ICO please visit [www.ico.gov.uk](http://www.ico.gov.uk)

<sup>10</sup> For more information on the consultation please visit <http://www.justice.gov.uk/consultations/misuse-personal-data.htm>

2.18 The DHR obliges government departments to carry out Privacy Impact Assessments (PIAs) on new projects or programmes involving significant amounts of personal data. The ICO has done significant work in promoting the use of PIAs across government through the provision of guidance and workshops. PIAs mean any proposal that involves the processing of personal data are considered early in the planning process, allowing any adverse impacts to be reduced or avoided altogether. Two hundred and seventy such assessments are now complete or underway across government, and departments are making sure that these processes are part of all procurements of IT systems or projects involving large amounts of personal data.

#### Clear accountability

- 2.19 The DHR introduced mandatory governance structures, and defined specific roles and responsibilities throughout government departments.
- 2.20 Accountability and the clear ownership of information risk at the top of organisations is vital in enabling good information risk management throughout an organisation. It is important because it makes clear who is responsible for the proper handling of data and who takes decisions about the management of risks to information.
- 2.21 Accounting Officers, and their boards, now regularly assess information risks and ensure there are robust plans in place to manage them. Information risk is also now included in the Accounting Officer's Statement of Internal Control.

### **Case Study 2.5: Ownership of information risk at board level**

#### **The Ministry of Justice**

- The Ministry of Justice has put corporate leadership at the heart of its Information Assurance agenda by creating a new Corporate Management Board sub-committee which is responsible for overseeing management of information risks at a strategic level and compliance with the requirements of the Data Handling Review.
- The committee has recently widened its remit to cover all aspects of knowledge and information with the aim of driving up capability and practice across the Ministry.

#### **The Home Office**

- The Home Office board and audit committee receive regular reports on Information risk, and the actions taken to manage those risks.
- The Home Office has introduced a dedicated Information Assurance Business Advice Team to work proactively with business units in order to ensure the smooth, effective and safe use of information, making sure that information risks are managed whilst continuing to meet business need.

2.22 The DHR made mandatory the role of Senior Information Risk Owner (SIRO), leading on information risk at board level. An active network of SIROs from organisations across central government and other public bodies is now firmly and effectively established. The SIRO is responsible for owning the overall information risk policy and ensuring its effective use in the organisation, and for leading the cultural change necessary within organisations to ensure information is valued, protected, and used properly by all members of staff.

2.23 The SIRO is supported by a network of Information Asset Owners (IAOs) of whom there are now more than 9,000 in central government organisations. Because of the variety in the size and business of public sector organisations IAOs are necessarily different kinds of staff in different organisations. In most cases IAOs have direct managerial responsibility and access to the information that is held, and must know how it is used and by whom. They help make sure that information is accessed and used appropriately for the public good, and specify the controls that must be in place if information is to be transferred outside the organisation's direct control. Cabinet Office and CESG have provided guidance and support for departments on the role of the IAO.

#### Improving the tools for managing risk

2.24 There are many tools which can help manage the risks to information. These include; increased transparency, contractual measures, and formal assessment processes.

#### *Increased transparency*

2.25 Setting out a clear statement of the ways in which government uses information improves public understanding and helps clarify the expectations of the protections that should be in place.

2.26 In line with the mandatory requirement in the DHR, all central government departments have published Information Charters on their websites, setting out the standards that everyone can expect from the department when it requests or holds their personal information, how they can get access to their personal data and what they can do if they do not think that standards are being met.



## Case Study 2.6: Increased transparency- FCO and DfT

Information charters help make clear how government uses information.



### FCO Information Charter

**We need to handle personal information about you so that we can provide services for you. This is how we look after that information.**

When we ask you for personal information, we promise to:

- make sure you know why we need it
- only ask for information proportionate to what we need
- protect it and make sure nobody has access to it who shouldn't
- let you know if we share it with other organisations to give you better public services – and if you can say no
- make sure we don't keep it longer than necessary, and
- not make your personal information available for commercial use without your permission.

In return, we ask you to:

- give us accurate information, and
- tell us as soon as possible if there are any changes, such as a new address.

This helps us keep your information reliable and up to date.

You can ask for more information on:

- how to find out what information we hold about you and how to ask us to correct any mistakes
- agreements we have with other organisations for sharing information
- our instructions to staff on how to collect, use and delete your personal information
- how we check the information we hold is accurate and up to date, and
- how to make a complaint.

FOR MORE INFORMATION, PLEASE CONTACT:

([dp-foi.img@fco.gov.uk](mailto:dp-foi.img@fco.gov.uk))

In abiding by these commitments, we will keep to the law, including the Data Protection Act 1998 and the Freedom of Information Act 2000. For independent advice about data protection, privacy and data-sharing issues, you can contact the Information Commissioner at: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Phone: 08456 30 60 60 or 01625 54 57 45 Fax: 01625 524510 Website: [www.ico.gov.uk](http://www.ico.gov.uk)

### The Department for Transport

In publishing its Information Charter, the Department for Transport also provided details of its information sharing activities. This allows the public to see what information is shared, with whom and for what purpose.

2.27 In addition, as of 2007/08, all central government departments have published details of any significant data incident in their annual resource accounts.

2.28 Should a loss or compromise of information occur, departments are now required to have a process to ensure that it can be dealt with as speedily and efficiently as possible. These processes focus on reducing any risk to those involved, minimising any impacts, swiftly learning lessons and implementing change where necessary.

#### *Contractual measures*

2.29 Government works in partnership with many organisations in order to deliver public services. But when information is transferred between organisations it must be properly protected regardless of which organisation handles it.

2.30 In many cases contracts form the basis of the understanding between organisations and so provide a powerful way to ensure that there is a clear common view of the standards that should be in place to protect information.

2.31 Following the DHR, the Office of Government Commerce (OGC) updated its model contract for ICT services<sup>11</sup>. Over 2,000 government contracts now contain these clauses, which strengthen the requirements for suppliers handling data on behalf of government.

#### *Government suppliers*

2.32 Private sector organisations increasingly recognise the commercial and reputational risks that they run if information is not handled properly. Because they handle government data, it is particularly important that suppliers to government have robust protection and management of information risk in place.

#### **Case Study 2.7: Data handling in government suppliers**

- The Home Office have introduced a supplier self-assessment tool which is designed to reduce the risk of loss of sensitive information in the supply chain. The tool is called 'Helping Assess Data Risk & Information Assurance Nationally' (HADRIAN). It comprises an online questionnaire, reporting module and internal process covering supplier engagement and audit.
- Hewlett Packard has brought in 10,000 licences for the government produced data handling e-learning package. Furthermore, EDS (a HP company) have implemented a security improvement programme with clear roles and responsibilities at the top of the organisation and throughout, mirroring arrangements in government. The programme has already put in a regime of regular security inspections, training, and a mandatory encryption of removable media such as laptops and USB memory sticks and is delivering good practice based on the ISO 27001 standard, and CESG advice.
- Fujitsu have 140 specialist staff that ensure that systems are designed, built and operated securely. The whole of Fujitsu's UK and Ireland workforce (12,000 people) have been given information security training to ensure that the importance of protecting government data is understood. This training is monitored by senior staff and further training is being developed. Fujitsu are also encrypting every laptop in the organisation to the same standards set out in the DHR, or higher where required.

Further information on the work being done to improve data handling in suppliers to government can be found at [www.intellectuk.org/ISAB](http://www.intellectuk.org/ISAB).

2.33 The improvements made by suppliers represent an important step, but more remains to be done in ensuring that the same standards set by government consistently apply in those organisations handling data on behalf of government.

2.34 In addition to the contractual measures that the DHR set out, Cabinet Office, in partnership with Intellect, have been working together with key ICT suppliers to ensure a clear and common understanding of government requirements, and that those requirements develop in a mutually beneficial and coordinated way. The HMG Information Security and Assurance Board are addressing supplier assessment, performance, and education and training. A key aim of the group is to

---

<sup>11</sup> The recommended Government standard for ICT enabled business change projects. There are now over 6,000 registered users of the ICT model contract.

develop common tools and processes for ensuring that government's commercial partners are aware of government requirements in protecting the personal data they may handle on behalf of departments.

#### *Setting the direction of change*

- 2.35 In order to sustain and develop the progress made by the DHR, CESH and Cabinet Office have introduced the Information Assurance Maturity Model (IAMM) as a way of helping organisations understand their strengths and weaknesses in information handling, and to set out the path to improvement over the longer term.
- 2.36 The IA maturity model includes all of the DHR measures as well as actions for longer-term improvement, and focuses on 6 areas:
- Leadership and Governance
  - Training education and awareness
  - Information risk management
  - Through life measures
  - Assured information sharing
  - Compliance
- 2.37 Departments will report to Cabinet Office annually on each of these areas allowing a picture to be built up of the risks that departments face; best practice to be identified; and areas which require improvement to be addressed. This process will also help inform future reports to Parliament on information risk in government

#### **Ensuring the right technology is available to protect information**

- 2.38 New technology is part of the reason that government and other organisations face new kinds of risk. For example, as the number of people working on the move and at home grows, so does the demand for new technologies to accommodate new ways of working. But technology can also help reduce the risks that new ways of working can bring. One of the mandatory measures of the DHR is the encryption of removable media that contains personal data. This means that if an encrypted laptop or USB memory stick is lost or stolen then the data, and any individuals it relates to, are protected. Departmental reporting indicates that the use of encryption is now widespread with over 100,000 devices now encrypted.

#### **Case Study 2.8: The National Technical Authority for Information Assurance**

CESH has a crucial role in supporting government and the wider public sector in making sure that risk and vulnerabilities are understood and that the right technological solutions are in place. Substantial progress in this area has been made. CESH's has expanded its capacity to provide additional services to government and, in concert with Cabinet Office and CPNI, IA policy, threat assessment and good practice guidance is constantly refreshed to ensure that information can be both used and protected effectively.

CESH also help identify areas of common technical requirements across government and ensure that these are coordinated and effective; and then work with Industry on solutions.

- 2.39 Enhanced technical measures can make routine business low-risk. But they may also imply new kinds of risk, and government cannot afford to underestimate the growing external threats to its systems. The DHR mandated the use of Penetration Testing where systems process large numbers (100,000 or more) of identifiable individual records. These tests use CESG approved independent experts to test the security of government systems. Over 600 independent penetration tests are now underway or completed across government.

### **Case Study 2.9: HMRC Managed Data Transfer Service (MDTS)**

The MDTS helps HMRC safely transfer both physical and electronic data. It is a system which logs monitors and controls when data is transferred within and outside HMRC, why, and who manages the process. It will provide stronger scrutiny and greater transparency in the way HMRC uses and manages information.

It can manage requests ranging from sending CDs, removable drives, USBs, floppy disks, DVD's etc. to large scale electronic transfers of information between HMRC and other government Departments. Roll-out started in October 2008 and when fully implemented the MDTS will:

- Reduce the risk of data loss associated with the physical transfer of data using couriers
- Provide a system of control requiring evidence that approval (and appropriate challenge) has been obtained for each data movement
- Ensure that media movements are processed through standard repeatable processes, enabling the Department to ensure effective controls are in place and to improve the efficiency of data movements
- Improve delivery tracking and auditing of movements through centralised logging and reporting.

### *Accreditation*

- 2.40 Accreditation is the process of independently and rigorously testing the protections in place for information systems against a demanding set of government standards. The DHR mandated the accreditation of all systems that carry information that is protectively marked if there are any significant changes to those systems, or at least every 5 years. This is helping to ensure that there are consistently high standards of technical protection and risk management in place for government systems.

### **The wider public sector**

- 2.41 Most public services are delivered by organisations outside central government; the wider public sector.

### **Case Study 2.10: Organisational culture in the wider public sector**

The wider public sector is often at the frontline of the delivery of public services. From the payments of benefits to the handling of medical records, the wider public sector handles a great deal of information. These are some of the measures that have been put in place so far:

#### **Local Government**

- The Local Government Association in partnership with the Society of IT management (SOCITM) is driving forward a programme of improvements in local government which are designed to closely correspond with the measures already in place in central government.
- Each Local Authority should now have its own IA strategy in place, and further work is also in progress to help support the development of the skilled people needed to deliver and sustain improvements in data handling.

#### **The NHS**

- The Department of Health has built upon its existing information governance framework to ensure that NHS bodies are clear about expected standards which are aligned with those applicable to central government.
- Performance management arrangements have been put in place to drive improvements where the required standards are not met.
- Where necessary, contracts with various organisations are being renegotiated to make sure the right protections and standards are in place.
- The National Programme for IT in the NHS is replacing older computer systems with modern systems that have state of the art security.
- Nearly 1 million encryption licences have been taken up for free by the NHS under a nationally negotiated contract that has delivered considerable cost savings.
- Online training has been made available to over 1 million staff at no cost to individuals or their organisations.

#### **The Police**

- Substantial progress has also been made within policing. Security policy has been altered to correspond with the measures put in place by the DHR, and has been reissued to all police forces.
- The assessment of compliance with policy is also now aligned with the system in place in central government and this will allow forces to establish clear standards for performance and improvements in data handling.

2.42 Central government is committed to a constructive relationship with the wider public sector in securing effective and efficient public services and offers advice and guidance in how to manage information risks. Wider public sector organisations such as local government bodies, the NHS and police, remain responsible for the services they deliver and the information risks that arise in doing so.

2.43 The changes described will improve the handling of information in the wider public sector. It will be important to sustain and build upon this progress to help make sure

wider public sector organisations meet the information risk challenges they face, and ensure there is appropriate correspondence with the measures set out in central government. This is necessary if, when information is shared in the public interest, there are to be clear and common expectations as to the protection that information must be afforded.

- 2.44 Central Government will continue to consult with those responsible for improving data handling in the wider public sector to encourage progress.

### **3 Looking to the Future**

- 3.1 The DHR has ensured that a great deal of progress in protecting information in government has been made in a relatively short space of time. It has mobilised staff in the hundreds of thousands to receive enhanced training in data security, encrypted devices and put in place new means for monitoring and scrutinising compliance with the new requirements. A sound framework for how government departments handle and protect personal information is now embedded and can be built on as necessary.
- 3.2 Technological change and the increasing sophistication of external threats mean that the risks to information will continue to evolve and increase in scale. Improving the ways in which information risks are managed will consequently always be an ongoing task and government must continue to monitor and improve guidance and procedures as necessary.
- 3.3 This section sets out the issues and actions that will be important in meeting these future challenges, which can be split into 3 areas:
- Sustaining the change
  - Coordination
  - Long-term risks

#### **Sustaining the change**

- 3.4 The changes made by the DHR are significant. Making sure that this progress continues will mean continuing to focus on getting the right organisational culture, making sure that the management of information risk remains well integrated in the every day business of government, and continued work with delivery partners.

#### *Organisational culture*

- 3.5 Changing organisational culture takes time. While there has been substantial progress in creating the right culture this will always need to be maintained and developed.
- 3.6 Many lessons have already been learnt in implementing this change; identifying and sharing best practice will be an important step forward. Monthly SIRO seminars held at the Cabinet Office act as an important conduit for transferring best practice and information between government departments.
- 3.7 It will also be necessary to refresh and develop training programmes to ensure they remain relevant and engaging. New targeted tools to help drive cultural change further are also emerging and taking full advantage of these must be a priority in an environment where resources will be under increasing pressure. Those leading the cultural change within departments must ensure that information risk remains an issue that staff are aware of and understand.

*Ensuring that information risk management is integrated with the business*

- 3.8 Information risk and the protection of data do not exist in isolation. The use of information by government is always in support of delivering better, more efficient public services.
- 3.9 For this reason, the management of information risk must continue to be integrated into the mainstream business of an organisation. The DHR requirement for board level ownership of information risk is an important step forward in this respect. This effort must be sustained with a continued focus on education and professionalism to ensure that data handling training remains embedded in core training. The expertise and skill of HR professionals and auditors will also be important in continuing to make sure that information risk is considered throughout the business and from the outset. Further work is being done with the OGC to ensure that IA is embedded within the Gateway Review process for major government projects and programmes.

*Working with delivery partners*

- 3.10 Government organisations will continue to rely on complex delivery chains in order to deliver public services. Where this means that personal data must be shared, the public will rightly expect that their information will be protected.
- 3.11 The progress already made by central government in implementing improvements shows that there is a way forward in achieving high standards throughout the delivery chain and a mutual understanding of, and approach to, information risk. This will include the formation of an agreed assurance approach for meeting government IA requirements under the overall guidance of the National Information Assurance Strategy (NIAS). This work will continue and be expanded to include suppliers and the wider public sector.

**Coordination**

- 3.12 As information is a key asset for all organisations, information assurance must be an essential consideration for all government work that touches on the use or protection of information. This includes both specific initiatives and investments. In order to meet the challenge of a continually changing set of risks to information, Cabinet Office will continue to coordinate the work done across government with implications for information risk management. This includes work in support of:

*The National Information Assurance Strategy*

- 3.13 The National Information Assurance Strategy was first published in 2003 and updated in 2007 with the aim of creating “A UK environment where citizens, businesses and government use and enjoy the full benefits of information systems with confidence.”
- 3.14 The NIAS is being updated and refreshed to reflect the progress made by the DHR and other relevant changes in the delivery environment. The updated NIAS will be published in 2010.



### *The Cyber Security Strategy*

- 3.15 The Cyber Security Strategy<sup>12</sup> was published in June 2009 in order to ensure that “Citizens, business and government can enjoy the full benefits of a safe, secure and resilient cyber space: working together, at home and overseas, to understand and address risks, to reduce the benefits to criminals and terrorists, and to seize opportunities in cyber space to enhance the UK’s overall security and resilience.”
- 3.16 The Cyber Security Strategy is focussed on reducing the risk from the UK’s use of cyber space especially ensuring sustainable UK IA capability; understanding and defending against adversities and vulnerabilities in cyber space; and, improving knowledge, capabilities and decision-making. Where relevant, the work in this area will be fully integrated into the updated NIAS.

### *The Digital Britain Report*

- 3.17 The Digital Britain Report<sup>13</sup> was published in June 2009. Digital Britain aims to secure the UK’s position as one of the world’s leading Digital Knowledge economies, recognising that the digital world is now a reality in all our lives.

### *Power in People’s Hands: Learning from the world’s best public services*

- 3.18 The Power in People’s Hands report<sup>14</sup> was published in July 2009. The report addresses the need for UK public services to innovate rapidly and to learn from the best services around the world.
- 3.19 The use of technology and information systems to achieve these goals runs throughout the proposals in the report. The range of uses of information run from the provision of information to new ways for service users to contribute; to service design and comment on public service performance.

### *Power of Information Taskforce Report and Making Public Data Public*

- 3.20 The Power of Information Taskforce Report<sup>15</sup> was published in February 2009 and aims to look at the ways in which government can improve its use of digital technologies and information. The Making Public Data Public initiative will deliver improved access to public information both in central government and the wider public sector.

### *Information Matters*

- 3.21 Information Matters<sup>16</sup> was published in November 2008 by The National Archives. The strategy addresses the importance of information to public bodies, how

---

<sup>12</sup> [http://www.cabinetoffice.gov.uk/reports/cyber\\_security.aspx](http://www.cabinetoffice.gov.uk/reports/cyber_security.aspx)

<sup>13</sup> [http://www.culture.gov.uk/what\\_we\\_do/broadcasting/6216.aspx](http://www.culture.gov.uk/what_we_do/broadcasting/6216.aspx)

<sup>14</sup> <http://www.cabinetoffice.gov.uk/strategy/publications/world-class-public-services.aspx>

<sup>15</sup> [http://www.cabinetoffice.gov.uk/reports/power\\_of\\_information.aspx](http://www.cabinetoffice.gov.uk/reports/power_of_information.aspx)

<sup>16</sup> <http://gkimn.nationalarchives.gov.uk/gov-strategy.htm>

capability to manage information can be developed further, and how management of knowledge and information will be improved.

#### *Frontline First: Smarter Government*

- 3.22 Published in December 2009, Frontline first<sup>17</sup> sets out the government's approach to the challenges of the next decade. It sets out actions to: strengthen the role of citizens and civic society; recast the relationship between the centre and the frontline; and, streamline central government for sharper delivery.
- 3.23 Each of the policy initiatives in this section will involve use of information or will affect the way that information is protected. The updated NIAS will set out the relationships between the elements of each of these pieces of work that relate to the protection and exploitation of information.

#### *Collaboration and ensuring value for money*

- 3.24 As well as specific initiatives, it is also important to coordinate investment with relevance to information risk in the interests of the 'common-good' across government.
- 3.25 Government already seeks to make sure that: when it makes investments in protecting information it does so in a coordinated way across departments; it makes sure that existing solutions are reused where possible; and ensures that new investments in IT enabled services are designed to have protection of information built in from the outset. This approach needs to be built upon to ensure that these benefits are achieved wherever opportunities to collaborate exist.

#### **Long-term risks**

- 3.26 Many of the risks to information used in government are long-term, and though there are mitigations in place, they remain areas where improvement must be sought. For example; control of access, paper records, and the need to continually improve information risk management of all kinds. Whilst the implementation of the DHR has meant substantial progress on each of these, there remain complex challenges where government will continue to seek improved ways to manage these risks in pursuit of the goals of the NIAS.

#### **Conclusion**

- 3.27 The cultural, procedural and technical measures put in place by the DHR have led to a substantial improvement in the way that government protects information. It is also clear that the landscape is continually changing and that we must adapt accordingly. The updating of the National Information Assurance Strategy in 2010 will address the next steps that must be taken in order to continue the progress made, and set the strategic direction.
- 3.28 A huge amount of work has been, and will continue to be, devoted to making sure the right protection for information is in place. There is no doubt that this task, and

---

<sup>17</sup> <http://www.hmg.gov.uk/media/52788/smarter-government-final.pdf>

keeping pace with change is and remains, challenging. The way that the Internet has changed and shaped society over the course of the last decade serves to highlight the importance of information, how it is held, transferred and used. It is certain that the future holds many great opportunities for public services in how it uses information to bring huge benefits to the public, the economy, and society as a whole and protecting that information is a challenge that we must meet.

## Annex A: Progress in Implementing the Minimum Mandatory Measures

Implementation of the minimum mandatory measures (MMM) is just the beginning of a process to ensure that IA measures are an integral part of routine business practice throughout government. The MMMs are blend of people, process and ICT measures. Analysis of the returns from 20 departments in 2009 showed that 99.1% of the MMMs had been implemented and have begun to embed in working practices in Departments and their delivery chains.

Those assessed below as 'Achieved' represent a single output or action that has been completed e.g. the naming of a SIRO. Others, for example Culture Change Plans, are more complex. For example they are initiated with a plan that takes time to implement and they require monitoring to test their effectiveness. These are judged as 'Building'. Those measures assessed as 'Established and Ongoing' indicate a process or a policy which has been established and continues to be applied or monitored as circumstances change or time elapses.

### Process Measures to Manage Information Risk

1. **Information Risk Policy:** Achieved - All Departments have developed IR policy or reviewed it where it already existed in the light of the DHR.
2. **Quarterly Risk Assessment in the Delivery Chain:** Building - Based on reporting in 2009 a number of initiatives are in train in departments to establish processes that assess IA compliance; some departments have established forums at which these matters are discussed with their delivery partners.
3. **Accredit ICT Systems Handling Protectively Marked Information:** Established and Ongoing - All new ICT systems that include the handling of personal or protectively marked information will be accredited. Those already accredited are subject to regular review.
4. **Conduct Privacy Impact Assessments (PIA):** Established and Ongoing - All new ICT projects that include personal data must now complete a PIA; guidance on the process is provided on the Information Commissioner's website. The PIA is also being applied to the development of new policies that encompass the handling of personal information.
5. **Use of OGC Model Contract Security Clauses:** Established and Ongoing - The OGC clauses are strengthening contractual arrangements on IA and are included in all new contracts that include the handling of personal information.
6. **IA Measures Adopted Across the Delivery Chain:** Building - In 2009 departments reported on the major Delivery Partners in their delivery chains; by the next reporting round a process will be in place to improve the assessment of 3rd Party Suppliers' IA compliance.
7. **Monitor Application of Measures to Protect Personal Information:** Established and Ongoing - departments have established compliance regimes that regularly monitor and report on the handling of personal information.
8. **Named SIRO:** Achieved - A strong SIRO community has been established supported by CO/CESG run SIRO seminars aimed at increasing awareness on key topics and sharing information on departmental IA projects.
9. **Identify Information Assets with named IAOs:** Building – Initial assessments of Information assets have taken place across government. Further work is in hand in partnership with The National Archives to improve consistency of approach across departments.
10. **Identify all Users of Protected Personal data:** Achieved - Records are maintained of those members of staff and contractors with access to or who are involved in handling protected personal data.
11. **Review Annually Use of Information Assets:** Building - Departments now assess their information assets in order to ensure the best use of information.
12. **Risk Assessment shared with Audit Committee:** Established and Ongoing - Risk assessments are regularly shared with departments' audit committees.
13. **Culture Change Plans:** Building - Departments have put in place training and cultural change programmes. Further work is underway to maintain the effort to foster a culture that values, protects and uses information for the public good.

14. **Monitor Progress through People Survey:** Established and Ongoing - A Pan Government people survey, with IA content, was sent out by Cabinet Office in October.
15. **Performance reflected in HR measures:** Established and Ongoing - Departments have made clear, in the relevant processes, that failing to apply controls when handling sensitive data is a serious matter that in certain circumstances may be regarded as gross misconduct.
16. **Process to Capture Individuals Information Risk Management Concerns:** Building - Through training, awareness and communications programmes staff are being made aware, of the processes in place to capture in confidence, and address, any concerns they may have on how personal information is managed.
17. **Incident Management Policy:** Achieved - Departments have developed, or reviewed existing, incident management policies in the light of the DHR requirements and shared good practice in the community.
18. **Consistent Incident Reporting:** Established and Ongoing - Widely and well communicated incident handling policy and processes within departments are now in place; enabling the identification of potential trends and good practice.
19. **Publish an Information Charter:** Achieved - Each department has published an Information Charter setting out the standards that people can expect when it requests or holds their personal information and what they can do if they do not think that standards are being met.
20. **Annual Report Return:** Achieved - Ministerial Departments and HMRC all submitted an Annual Report to the Cabinet Office.

### **Specific Minimum Measures to Protect Personal Information**

21. **Identify All Holdings of Protect Personal Data:** Achieved - Departments have identified the protected personal information that they or their delivery partners and 3rd party suppliers hold.
22. **Handle Data as PROTECT throughout the Delivery Chain:** Established and Ongoing - All the DHR mandated measures are routinely being applied to protected personal data while it is processed or stored within departments or their delivery chains.
23. **Apply Suffolk Matrix:** Established and Ongoing - Training on the correct handling of protected information has taken place and is ongoing in all Departments.
24. **Secure Remote Access to Protected Data:** Established and Ongoing - Departments have established processes for secure remote access to data using agreed standards and approved products.
25. **Protection of Removable Media:** Established and Ongoing - Departments have implemented the DHR requirements to encrypt personal information when in transit on removable media.
26. **Strong Protection for Unencrypted Media:** Established and Ongoing - In situations where encryption is not practical, i.e. full system back-up tapes used for disaster recovery or business continuity, Departments have instituted strong controls and monitoring on their movement, access and storage.
27. **Controlled Disposal of Paper & Media:** Established and Ongoing - Departments have implemented policies for the secure disposal of media and paper.
28. **Review of Measures for Handling Protected Information:** Established and Ongoing - Departments have reported on the effectiveness of the DHR measures. Further compliance testing is ongoing.
29. **Penetration Testing of ICT Systems:** Established and Ongoing - Departments have conducted more than 650 Penetration Tests, and continue to work to ensure that testing is in place for existing and new systems.
30. **Information Risk Awareness Training:** Established and Ongoing - All Departments have trained those handling personal information in IA awareness. In the majority of cases departments have chosen to go further and extend this training to all their staff.
31. **Define Access Controls to Protected Information:** Achieved - Access rights to protected personal data have been defined to, where possible, minimise the number of records viewed unnecessarily.

32. **Log & Monitor Access to Protected Information:** Established and Ongoing - Managers are now required to check on a regular basis the logged activity of data users accessing protected personal information.
33. **Have a Forensic Readiness Policy:** Achieved - Departments have produced forensic readiness policies describing processes for preserving and analysing data generated by an ICT system that may be required for legal or management purposes as part of the information asset audit process.