Review of information security at HM Revenue and Customs

Final report

Kieran Poynter

June 2008

Kieran Poynter

Review of information security at HM Revenue and Customs

Final report

June 2008

HM Treasury contacts

This document can be accessed at:

www.hm-treasury.gov.uk

For enquiries about obtaining the publication, contact:

Correspondence and Enquiry Unit
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

Tel: 020 7270 4558

Fax: 020 7270 4861

E-mail: public.enquiries@hm-treasury.gov.uk

Printed on 100% recycled paper.
When you have finished with it, please recycle it again.

ISBN: 978-1-84532-473

PU567

Contents

	Foreword by Kieran Poynter	1
I	Preface	3

PART 1: THE INVESTIGATION

II	*The Investigation* – Executive Summary	7
III	Background to *The Investigation*	13
IV	The circumstances leading up to the data loss	15
V	Overview of relevant policies and procedures	33
VI	Other organisational issues	37

PART 2: THE WIDER REVIEW

VII	*The Wider Review* – Executive summary	43
VIII	What has changed since the incident?	47
IX	What has *The Wider Review* found?	49
X	How have we gone about our work?	53
XI	What does good information security look like?	55
XII	How to get there – the strategy	57
XIII	Moving in the right direction – HMRC's new organisational structure	63
XIV	What are we recommending?	65
XV	What progress has HMRC made?	89

APPENDICES

A	Poynter Review terms of reference	95
B	Glossary of key terms and abbreviations	97
C	*The Investigation* approach	99
D	Organogram of relevant individuals in HMRC	101
E	Diagram of key events leading to the loss	103

Foreword by Kieran Poynter

Dear Chancellor,

Information security review at HMRC

I am pleased to submit my report. The report is split into two distinct parts:

- The first part, entitled *The Investigation*, provides a narrative of how the Child Benefit CDs were lost and a commentary on the causes of the loss.
- The second part, entitled *The Wider Review*, is more forward-looking and contains my recommendations on how to improve information security at HMRC.

Whether working on *The Investigation* or *The Wider Review*, my team has consistently had the full and constructive co-operation of HMRC staff and management. Their reaction to what could have been a disruptive review has been impressive and I would like to thank HMRC for the time that has been given and the openness of the interaction.

Yours sincerely,

Kieran Poynter
Chairman and Senior Partner of PricewaterhouseCoopers LLP

I Preface

I.1 This report contains high level findings and recommendations arising from my review of information security in HM Revenue and Customs ("HMRC"). The review was commissioned following the loss of two compact discs containing personal information about families derived from the Child Benefit Office ("CBO") computer system. My report sets out a detailed factual account of the circumstances giving rise to that incident in Part 1.

I.1 In Part 2, I describe the *Wider Review* I have conducted across HMRC. That part contains my principal findings of lessons to be learnt and high level recommendations for the future arising from both phases of the review. In the course of my work I also made several hundred detailed recommendations, many specific to individual Business Units. In the interests of security and brevity these are not included in this report. The terms of reference for the review as a whole can be found at Appendix A.

I.2 Though complementary, the two parts necessarily have different styles to them. *The Investigation* summarises a forensic analysis and is quite formal in tone whereas *The Wider Review* is written in a more conversational style and is intended to bring to life the findings and recommendations coming from my review without the need for specialist knowledge.

I.3 In adopting the language used by HMRC, I have inevitably used many abbreviations. A table giving the full titles for abbreviations used in both parts of this report can be found at Appendix B.

I.4 The data loss incident arose following a sequence of communications failures between junior HMRC officials and between them and the National Audit Office ("NAO"). The loss was entirely avoidable and the fact that it could happen points to serious institutional deficiencies at HMRC.

I.5 The two major institutional deficiencies from which many of the more detailed issues flow were:

- Information security simply wasn't a management priority as it should have been, and
- HMRC had an organisational design which was unnecessarily complex and crucially, did not clearly focus on management accountability.

I.6 Both of these issues have now been addressed, but a great deal of work will be required to bring HMRC up to and to sustain the world class standard for information security to which it now properly aspires. Much can be done in the short and medium term to establish and consolidate control, but in the longer term, investment is required in new systems. My report sets out recommendations which when followed will enable HMRC to achieve its ambitions. I am pleased to acknowledge the progress the Department has made in this area, which is reflected in sections VIII (What has changed since the incident?) and XV (What progress has HMRC made?) of this report.

I.7 In my view, this represents a great opportunity. Modernising work practices and the systems which support them should lead to significant efficiency gains as well as the restoration of the reputation of HMRC.

I.8 I am pleased to report that HMRC has accepted my findings and recommendations and has made progress on 39 out of 45 of them, implementing 13 of them. I understand that my findings and recommendations are consistent with those of Sir Gus O'Donnell arising from his cross-government review.

PART 1

The Investigation

II *The Investigation* – Executive Summary

OVERVIEW

II.1 My review team has undertaken a highly detailed analysis of the chain of events leading to the loss of the Child Benefit data in October 2007 and a full description of the work undertaken is contained within Appendix C of this report. This work has shown that more than thirty HMRC officials, from four different departments, and a number of NAO staff, played some part in the story. It has been a complex task to understand the intricacies of what took place, though there has been broad agreement of the parties involved as to the chronology of events.

II.2 My review team has concluded that there were a number of factors that contributed to the loss of the data, but it has not encountered any evidence of malice or knowing disregard for policy or procedure in any of the circumstances leading to this loss. Rather it was an unfortunate catalogue of inter-locking factors which, in their totality, triggered the events which unfolded. These factors can be characterised in two ways:

(a) Factors directly contributing to the loss which, by their nature, are very specific to the events in question; and

(b) General factors within HMRC, in particular within the four relevant departments, which are evidence of institutional deficiencies.

II.3 The specific factors directly contributing to the loss of the child benefit data, examined in greater detail in paragraphs II.5 to II.16 below, included:

(a) the setting of a precedent in March 2007 which created the conditions for the loss to occur in October 2007;

(b) the failure to clarify and adhere to the "Single Point of Contact" ("SPOC") protocol between HMRC and NAO;

(c) the prioritisation by HMRC staff of other considerations above information security risk concerns;

(d) the failure to recognise and pursue available data redaction options;

(e) appropriate authorisation neither being sought nor obtained for the release of the data concerned; and

(f) the use of insecure methods of data storage and transfer.

II.4 The general and more institutional factors within HMRC which created the environment in which the data loss could occur are examined in greater detail in paragraphs II.17-II.23 below. These have been identified by my team as including:

(a) weakness in specific information security policies;

(b) inadequate awareness, communication and training in information security; and

(c) a lack of clarity around the governance and accountability for data guardianship.

FACTORS CONTRIBUTING DIRECTLY TO THE LOSS OF THE CHILD BENEFIT DATA

The setting of a precedent in March 2007

II.5 The first discrete external audit of the CBO was undertaken by the NAO in 2006-07. It was during the execution of this audit that the Child Benefit Computer System ("CBCS") data scan was first provided in full to the NAO and taken off-site for audit purposes. It is clear that these events, culminating in the provision of two compact discs ("discs") containing this data to the NAO in March 2007, established a precedent which led to the subsequent loss in October 2007 of a similar data scan.

II.6 One of the most important precedents set by the March events was that the data was provided to the NAO in full, even though the NAO had only requested a large sample and had attempted to get sensitive data redacted. The reasons that this occurred are explained further in paragraphs II.9 to II.11 below.

Failure to clarify and adhere to the SPOC protocol

II.7 The Tax Credit Office ("TCO") had been audited on a number of occasions by the NAO in previous years. In order to ensure that the process ran smoothly, HMRC and NAO officials had agreed a communication protocol whereby **two** SPOCs within HMRC would co-ordinate the NAO's activities, one for the overall execution of the audit, and another to respond to day-to-day information requests. A similar protocol was agreed for the audit of the CBO. Indeed, the same HMRC staff that had managed the TCO's relationship with the NAO took over these responsibilities in respect of the CBO audit in 2006-07.

II.8 My review team has found that the SPOC protocol was somewhat informal and its existence not widely publicised nor agreed by the parties until the second audit in 2007-08. Moreover, even though specific HMRC staff members were named as being SPOCs in NAO's planning document for this second audit, there were a number of direct interactions between the NAO and other HMRC staff, some of which were unknown to the SPOCs. As a result the SPOCs were unable to marshal the information flows in all cases. The provision of the CBCS data scan in October 2007 was one such case.

Operational concerns placed ahead of security risks

II.9 During the course of events in both March and October 2007, several HMRC staff expressed concerns about the security implications of transferring large amounts of sensitive data to the NAO. Indeed, the NAO representatives also expressed a preference for receiving either a specific sample of the data or to have sensitive information removed from the records, albeit primarily to reduce the size of the data file. These concerns were not escalated to a suitably senior level within HMRC and the suggestion to remove sensitive information from the scan was thwarted by concerns over cost and resources.

Miscommunication and misunderstanding regarding data redaction options

II.10 In fact, there were a number of options for redacting and for reformatting the CBCS data on site at HMRC premises in Waterview Park and London. For instance, I have learned that the stand-alone computer at Waterview Park used by HMRC's Claimant Compliance department for

undertaking its sampling exercises contained software capable of producing the requested sample data at virtually no cost, but this option was not explored by HMRC staff.

II.11 The redaction option which was considered, namely requesting that HMRC's Knowledge Analysis and Intelligence (KAI) department manipulate the data, was intended to be discussed with the NAO. In particular, it was suggested by the SPOC in March 2007 and was due to be discussed at a meeting between KAI and NAO representatives on 14 March 2007. The SPOC did not communicate this intention to the NAO and, consequently, the NAO believed the meeting to have a different purpose. Through a further oversight the point was neither put on the agenda nor discussed at that meeting. As a result, this option was never fully explored and subsequently overlooked.

Appropriate authorisation was neither sought nor considered necessary for removal of data off-site

II.12 The question of what level of authority was required for the full CBCS data scan to be released was not considered by the parties involved. The NAO did not communicate fully its information requirements in audit planning documents and junior HMRC staff did not think to escalate the matter to a higher level, being unaware of HMRC guidance specifically requiring staff to seek authority of a senior manager before releasing data to the NAO. As a result, no Senior Civil Service HMRC official was asked to permit the NAO to take the data off-site to conduct its analysis, and no such HMRC official knew that this was envisaged.

II.13 This also raises the question of who had "ownership" of the CBCS data and would therefore have been able to provide authority for its release. My review team has found that, though the issue of data ownership had been discussed previously by HMRC management, it had not been resolved at the time of the data loss incident and confusion among HMRC departments as to where this ownership lay was a contributory factor in that loss. The issue of data ownership is explored further in paragraph II.22 below.

II.14 One of the reasons that no such authority was sought by junior HMRC officials involved in the data transfers was a general misconception at that level that the NAO had absolute authority to access any information within HMRC's custody and that HMRC officials had a duty simply to provide it. While the NAO must be allowed access to all the information it requires for the purpose of its audit, HMRC was entitled to ensure that data was provided in an efficient and secure fashion. Any such concerns on the part of junior officials were overridden by their misconception of the NAO relationship.

Insecure methods of data storage and transfer

II.15 The CBCS data in question was routinely downloaded by a third party mainframe operator on to two discs for the purposes of a compliance sampling exercise every six months. HMRC specified the medium for this download, its format and the use of a certain version of proprietary software with limited alphanumeric password protection. Given the amount of sensitive customer data on the discs and the portability of such a medium, this level of encryption was clearly insufficient to protect the information in the event that the discs were lost. HMRC's application of the protective marking system used by government departments in relation to information is discussed further in paragraph II.19 below.

II.16 The discs which were lost in October were sent to the NAO via the internal Tax Post system operated by third party logistics company TNT. This system was mistakenly believed to be

a secure and traceable system by the HMRC staff member concerned. In fact it was not a traceable system, and when the discs went missing they could not be traced. Unknown to that official, TNT also provided HMRC with a traceable delivery system which should have been used to comply with HMRC policy, which did require that an auditable delivery method should be used.

INSTITUTIONAL HMRC FACTORS CONTRIBUTING TO THE DATA LOSS

Information security policy and procedure could have been stronger and better communicated

II.17 HMRC has detailed policies and guidance around information security and the release of data to third parties such as the NAO. For instance, it has policies requiring that authorisation be obtained for information disclosure outside the organisation and stipulating the use of auditable delivery methods for removable computer media containing sensitive data. If these policies had been adhered to, it is likely that the data loss could have been prevented.

II.18 In the event, very few of the HMRC staff involved in this case were actually aware of the existence of such policies and guidance. Clearly therefore they were not adequately communicated across the organisation. Furthermore, staff found the policy difficult to access via HMRC's intranet. I note that HMRC has since introduced training and communications schemes addressing those issues.

II.19 The policies and guidance that were in place lacked the procedural detail to cover some of the factors contributing to the loss of the CBCS data. These could have been strengthened and enforced to cover key aspects of information security in a large and complex organisation such as HMRC. In particular, it was not stated HMRC policy or procedure to encrypt removable computer media, assign a higher protective marking to aggregates of sensitive records or to encourage the NAO to undertake its information review exercises on HMRC premises. I note that HMRC has since improved its policies in each of these specific areas.

HMRC people lacked sufficient awareness and training on information security matters

II.20 There was a general lack of awareness across HMRC Business Units, at least prior to the incident, of the importance of information security.

II.21 The officials involved in this matter had received little or no information security training since their induction into the organisation. I note that HMRC has since introduced a mandatory half-day Information Security Workshop for all staff. More details can be found in section VIII.

Lack of clarity governance, accountability and communication in respect of data guardianship

II.22 As outlined above, a specific contributory factor in the CBCS data loss was the failure to seek or obtain appropriate authority for the disclosure of the full set of data. One of the problems faced by the HMRC staff involved was that there was no clearly assigned data owner or guardian from which to seek this authorisation. HMRC had previously debated the assignation and scope of a data guardian role but without conclusion at the time of the incident. This situation has since been rectified.

II.23 The fact that no senior HMRC official was involved in the events leading to the data loss raises serious questions of governance and accountability. In my opinion, a suitably senior official should have been more clearly accountable for the relationship with the NAO to be certain that the NAO was provided with appropriate data in an efficient and secure manner.

III Background to *The Investigation*

III.1 On 20 November 2007, the Chancellor of the Exchequer made a statement to the House of Commons explaining that two discs containing HMRC's customer data in relation to the payment of Child Benefit had been lost. The data had been sent to the NAO in response to a request for information for audit purposes via HMRC's internal post system which is operated by the courier company TNT. The package containing the data was not recorded or registered.

III.2 The terms of reference for this review were published by HM Treasury on 23 November 2007 and can be found in Appendix A of this report.

III.3 My team has now completed a forensic examination of the available evidence. This part of my report covers the work undertaken by the *Investigation* Phase of the Review, outlines my understanding of the events leading to the loss of the discs containing the CBCS data, the relevant policy and guidance in place at that time, and the reasons why they failed to prevent the loss of the confidential CBCS data. An overview of the work conducted in the *Investigation* Phase is attached at Appendix C.

III.4 In addition to the work carried out by this Review, the Metropolitan Police Service and the Independent Police Complaints Commission ("IPCC") have also been investigating this matter. The objective of the Police investigation was to reduce the potential harm to the general public that could be caused by the loss of the CBCS data. It was therefore focused on the data loss as a public protection issue, and in particular on seeking to locate the missing discs. The Metropolitan Police has since announced, as published in media reports on 15 January 2008, that its investigation to locate the discs was being wound down but not concluded.

III.5 The IPCC has a statutory independent oversight role in respect of public complaints and conduct matters relating to HMRC. I understand that this matter falls outside the mandatory criteria under which HMRC is required to refer matters to the IPCC. However, HMRC has referred this matter to the IPCC on a voluntary basis. The IPCC investigation is intended to establish whether there was any potential misconduct and what organisational learning emerges from the events leading up to, during and immediately after the loss of the discs. It is part of the IPCC remit to consider whether any disciplinary action is required and whether the steps taken by HMRC after the discovery that the discs were missing were appropriate and sufficient.

III.6 Given the need to examine the same set of facts, my team has co-operated with the IPCC to the fullest possible extent in conducting its investigation. This included conducting interviews in conjunction with IPCC staff, sharing working papers and evidence exhibits, and enabling the IPCC to utilise my office premises and equipment from time to time to undertake forensic analysis of email and other electronic data. I have shared the contents of this report with the IPCC to ensure that its analysis of events is consistent with mine.

III.7 In the course of our investigations, we have also engaged in a dialogue with the NAO. Though that organisation is not specifically covered by the Review's terms of reference, its interaction with HMRC lay at the centre of the events leading to the loss of the CBCS data. The NAO has co-operated fully with my team in providing its own account of these events, supplying supporting documentation to this account, and submitting its staff for interview. However, the NAO has not been subject to the full forensic analysis conducted by my team at HMRC. In spite

of this, I have identified no cause to believe that any material findings would have been significantly different had such a forensic analysis been conducted by my team at the NAO.

III.8 To protect the identities of HMRC and NAO staff, and others, who have cooperated with my team, the names of individual HMRC and NAO staff members involved in the circumstances leading to the loss of the CBCS scan discs are not included in this report.

III.9 I also note that the Information Commissioner has independent statutory functions directed at promoting compliance with data protection legislation. The Chancellor's Parliamentary statement of 20 November 2007 confirmed that the Commissioner had been informed and consulted about the data loss incident and that a full copy of my report would be made available to the Commissioner. For his part, the Commissioner indicated then that "searching questions" needed to be answered, but that – rather than launch his own investigation – he would decide his approach in the light of this Review. The Commissioner has been kept informed about progress, has been supplied with a pre-publication draft of this Report and (in accordance with my terms of reference) has been consulted about my recommendations. The Commissioner has indicated that he is satisfied that my Review has investigated all the facts and issues with which he needs to be concerned and that he fully supports all my Recommendations.

III.10 The Commissioner has informed me that he considers that my Report confirms beyond doubt that HMRC has breached the 7th Data Protection Principle, which requires appropriate technical and organisational measures to be taken against accidental loss of personal data. He has informed me that, accordingly, he proposes as soon as possible to serve an Enforcement Notice on HMRC under section 40 of the Data Protection Act 1998. The Commissioner envisages that the "specified steps" in such a Notice will – with a view to ensuring full compliance with the 7th Principle - require HMRC to use its best endeavours to give effect to the Recommendations of this Report. It is envisaged by the Commissioner that the Notice will go on to require HMRC to publish progress reports after 12, 24 and 36 months documenting in detail how the Recommendations have been, or are being, implemented to achieve that compliance.

III.11 It should be noted that prior to the commencement of the Poynter Review, PricewaterhouseCoopers LLP ("PwC") had been asked by the NAO to assist them in their auditing of the CBO in 2007-08 and beyond. Specifically, due to resource constraints NAO had asked for PwC's assistance in testing various controls within the CBO, rather than any wider assurance work. For the avoidance of doubt, none of the testing related to controls over information security. In addition PwC was not to have any responsibility for the selection or extraction of samples from HMRC data or for its method of transmittal to the NAO. As a result of the NAO's request, PwC staff did become involved in the early stage planning work for the CBO audit in October 2007 and the programme of work was discussed and agreed with them in early November 2007. Samples for controls testing (approximately 325 transactions/cases) were provided to PwC by the NAO in early November and PwC representatives commenced work on site at the CBO on 13 November 2007. In order to avoid any perception of conflict of interest, this work was halted and discontinued on 20 November when I was appointed to conduct this review. Both HMRC and HM Treasury were made aware of PwC's limited involvement in the early stages of the CBO audit and shared my conclusion that it did not represent a conflict of interest.

IV The circumstances leading up to the data loss

INTRODUCTION

IV.1 The events leading to the October 2007 data loss involved a number of Business Units within HMRC as follows:

(a) The Benefits and Credits Business Unit ("B&C") which oversees the whole process of Child Benefit and Tax Credits from initial application through processing, recording and payment. Benefits & Credits includes both the CBO and the TCO;

(b) The Information Management Solutions (IMS) which is responsible for the management of the CBCS. Data processing is outsourced to Electronic Data Systems ("EDS"), a third party supplier. In simple terms, the Child Benefit data is the property of HMRC while the computer equipment on which it is stored and processed is owned by EDS. Requests for data from the CBO are directed to IMS, who manage the retrieval of that data from EDS;

(c) The function of the Claimant Compliance (CC) Business Unit is to investigate and seek to prevent fraudulent Child Benefit claims. To assist them with their work, CC is provided with a complete download of the data contained in the CBCS every six months, in March/April and September/October. IMS requests this data on behalf of CC by completing a User Requirement and Acceptance Criteria document ("URAC"), which specifies the scope of the data to be provided, the format and the method by which it is to be transferred. The data is provided by EDS to IMS on two discs and IMS in turn passes these discs to CC. The information is then transferred by CC from the discs on to a stand-alone computer which is contained in a room at the HMRC offices in Washington, Tyne & Wear, which is secured by an entry code and alarmed; and

(d) KAI, a Business Unit which undertakes statistical analysis and sampling exercises of HMRC data, and manages organisational surveys such as the HMRC staff survey. Notably, KAI is involved in overseeing the annual random review sampling undertaken by CC.

IV.2 The organogram at Appendix D to this Report sets out the staffing structure of each of the above Business Units and the extent to which they are interrelated.

IV.3 The other main party involved in the events is the NAO. As outlined on its own website, the NAO scrutinises public spending on behalf of Parliament. This role entails auditing the accounts of all central government departments and agencies, as well as a wide range of other public bodies, and reporting to Parliament on the economy, efficiency and effectiveness with which they have used public money.

IV.4 Discs containing a download of the data contained in the CBCS were transferred to an auditor from the NAO on two occasions, in March 2007 and October 2007. In order to understand fully the events leading to the data loss in October 2007, my team has also examined circumstances surrounding the March 2007 transfer, which set a precedent for what took place in October. The events leading to each transfer are outlined in chronological order below. The key events in this chronology are also depicted graphically at Appendix E to this Report.

IV.5 The staff grades of those aware of provision of the discs containing the CBCS data to the NAO include "Senior Officer", "Manager", "Higher Executive Officer", and others which to the uninformed reader may suggest a high level of seniority within HMRC. These are administrative grades and none of those aware of the situation were members of the Senior Civil Service within HMRC.

THE MARCH 2007 TRANSFER

The planning of the 2006-07 audit

IV.6 It should be explained from the outset that 2006-07 was the first occasion on which the NAO undertook a separate, discrete audit of the CBO, though it had undertaken an audit of the TCO on a number of previous occasions. The start of this external audit of the CBO and its resulting information requirements provide the background to the removal of the data in question in March.

IV.7 On 24 October 2006, NAO Employee1, a Director of the NAO, sent a letter to an HMRC Commissioner, outlining the audit approach for the financial year ending 5 April 2007 and attaching a 2006-07 Resource Accounts Audit Strategy document. This document sets out the high level objectives of the audit and the planned approach that the NAO would follow. It does not go into detail as to the information requirements of the audit nor the method of transfer of information between the parties. In his interview, NAO Employee1 explained that the NAO 2006-07 audit of HMRC was affected by the introduction of ISA (International Standard on Auditing) 315, "Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and Its Environment" and a new NAO financial audit manual introduced that year. The impact of those changes was that the planning materiality for the audit was reduced from £150m to £75m. However, NAO were aware of the results of an appraisal conducted by HMRC which indicated a level of error within Child Benefit payments (potentially as much as £100m). The NAO were also aware of the fact that the so-called "random review programme" conducted by HMRC (which tested "closed" cases only) did not actually select its sample on a truly random basis. As a result, and in light of the fact that the potential error (identified in the HMRC report) exceeded the new materiality level, the NAO decided to go beyond their planned re-performance of HMRC testing. On 23 February 2007 NAO took the decision to "independently sample". This meant that NAO would randomly select its own sample for testing purposes. The decision to "independently sample" was subsequent to the production of the audit strategy as articulated to HMRC. There was no formal communication from NAO to HMRC of this change in audit approach. In a letter to HMRC dated 9 November 2007, after the discs had gone missing, NAO Employee1 noted *"We signalled the change in our audit approach in our 2006-07 Resource Accounts Strategy, though without being explicit about the additional substantive testing that we proposed, nor addressing how we might extract this data."* He goes on, *"..having redefined the direction of our audit approach for Child Benefit Awards, I should have personally ensured that, as data owner, you were fully apprised of what we planned to do; and what access we would need to the Child Benefit data. I should also have ensured that the Finance Director was also appraised of and understood the implications of the change in audit approach. Neither of these contacts happened and I apologise unreservedly for the fact that I did not give you (both) the opportunity to discuss with us how we might be able to sample Child Benefit data; and carry out the other analysis that we had envisaged on the awards."*.

IV.8 The Lead Auditor with the NAO ("NAO Employee2") was tasked in October 2006 with the planning and supervision of the NAO's audit of the CBO. As one would expect, NAO

Employee2 therefore played a central role as the main NAO liaison with HMRC in both March and October 2007. One of NAO Employee2's first actions in this role was to send an email, on 5 December 2006, to EmployeeA, the Director and process owner for Benefits and Credits at HMRC, requesting meetings with various staff at HMRC's Water View Park offices in Washington ("WVP") in order to update the NAO's understanding of the Child Benefit system. In this email, NAO Employee2 stated that the former NAO auditor, for the audit of the TCO, had informed him that EmployeeA was the overall SPOC for such work.

IV.9 As a result, on 7 December 2006, EmployeeB, an Executive Officer in the Benefits & Credits Business Unit, sent an email to various recipients explaining that NAO Employee2 was planning to visit WVP for initial meetings on 12 December 2006, followed by meetings with named individuals on 14 December 2006. EmployeeB noted in her email that NAO Employee2 had a *"particular interest in electronic claims so I have extended the time in the claims area slightly to allow for this."* My review team has not found any evidence to suggest that the request for the March data transfer was raised by the NAO at this early stage of the audit.

The SPOC confusion

IV.10 My review team has identified that there were in fact two "SPOC" roles for NAO liaison in both March and October 2007. This distinction, and its communication to the parties involved, has significance in determining whether the correct channels were used for the data transfers. As outlined above, EmployeeA held the overall "primary SPOC" role, but he was assisted for day to day information and meeting requests by a more junior member of staff. For clarity in recounting these events, this more junior role will subsequently be referred to as the "secondary SPOC". My review team has not identified a document specifying the identity and responsibilities of the SPOCs for the 2006-07 audit. However, these were clearly set out in the draft Child Benefit Audit Plan for 2007-08 which stated that *"EmployeeA – the Child Benefit Process Owner – will continue to be our main liaison point for co-ordinating our audit work on Child Benefit. EmployeeC will take the lead in managing responses to our central requests for information".* It should be noted that this document was not widely distributed around HMRC and whilst there was a general awareness within the organisation of the existence of a SPOC role, my team has encountered limited internal understanding or guidance as to its definition or designation. The only such guidance identified had been an internal document, provided at interview by the secondary SPOC for October, entitled "Chapter 3: The role of the NAO Liaison Team" which states: *"The primary role of the NAO Liaison Team is to act as the main point of contact for the National Audit Office in the co-ordination of their work within the Department. They aim to improve communication and understanding between the Department and the NAO audit teams"*. The guidance goes on to list example activities to be undertaken by the liaison team but does not confer any authority or decision-making powers on either SPOC role, nor does it actually use this terminology.

IV.11 The secondary SPOC for the March transfer was EmployeeD, a Senior Officer in the Benefits & Credits Business Unit at HMRC. EmployeeD explained at interview that she had also acted previously in a similar capacity with regard to the NAO's audit of the TCO, hence the rationale for her taking on this role for the CBO. On 8 December 2006, EmployeeD sent an email to NAO Employee2, copied to EmployeeB and EmployeeA, in which she clarified the position regarding her role as secondary SPOC for NAO liaison, stating "*Can I ask you to send any requests for additional information or contacts relating to ChB to me please as the first point of contact".* EmployeeD has stated that she carried out the role of secondary SPOC for the NAO from May 2006 until March 2007, after which time, the role passed to EmployeeC, also a Senior Officer in the Benefits & Credits Business Unit. EmployeeD's role as the contact for information requests for the 2006-07 Child Benefit audit was noted in at least two other emails sent to the NAO, one sent

by EmployeeA to NAO Employee1 on 8 January 2007, and copied to other NAO staff, in which he noted that to be able to *"track all your [NAO] requests and ensure that what you require is delivered promptly will you please also copy EmployeeD into messages on the ChB audit work"*.

IV.12 My review team has found that whilst EmployeeD acted as the secondary SPOC in relation to the 2006-07 audit, other individuals also had contact roles for their Business Units, and communications between HMRC and NAO did not always flow through the same individuals. For example, in email communications, EmployeeE, a Grade 7 manager within CC, appears to have acted as the contact for that Business Unit, while EmployeeF, a Higher Executive Officer in IMS, was its main liaison person for the NAO relationship. EmployeeF has informed my team at interview that his specific contact at the NAO was NAO Employee3, adding that he did not generally liaise with NAO Employee2, as his requests were typically executed by EmployeeD. In interview, NAO Employee2 commented that *"it wasn't normal to have a single point of contact but it was usual to have key contacts who requests would be made from."* NAO Employee2 further added that he was not aware of any official guidance requiring a SPOC. The amount and frequency of these other interactions between the organisations in both March and October 2007, and the failure to adhere more rigidly to the designated communication channels may well have been contributory factors in the eventual data loss.

The NAO's initial request for information

IV.13 The first request for relevant information from the NAO was outlined in an email dated 5 March 2007 from EmployeeD to EmployeeA (copied to EmployeeB). EmployeeD recounted the details of a telephone call from NAO Employee2 on 1 March 2007 in which NAO Employee2 made the following requests:

(a) That the meeting with EmployeeE on 14 March be moved to London as the NAO wanted to *"bring along their statisticians to discuss sampling approaches and sizes"* [relating to the random review samples undertaken by the CC]. EmployeeD indicated in her email that KAI representatives would also be attending the meeting; and

(b) That details of all new and terminated cases for the full year (approximately 600,000 to 800,000 cases) be provided. The email indicates that NAO Employee2 wanted to undertake a "*secondary sampling exercise…*" and wanted to know "*how long it would take and in what format"* the data would be. In his interview EmployeeA explained that NAO Employee2's original request was in fact for between 1,200,000 and 1,600,000 cases, representing 600,000 to 800,000 for each of the year's new and terminated cases.

IV.14 The meeting scheduled for 14 March 2007, or more importantly the purpose, attendees and agenda for that meeting, assume greater significance later on in the chronology of events. However, it is first crucial to understand how NAO Employee2's initial request for information outlined in paragraph (b) above ultimately evolved into the transfer of the entire CBCS scan to the NAO. The first clue lies in EmployeeD comments in the same email dated 5 March 2007 that *"I've done a lot of digging and we can supply the majority of his demands, at nil cost (Compliance have just recently done a 100% scan on live load so they could use that). If this hadn't been available it would have cost a fortune and have taken weeks."* At interview, EmployeeD explained that she had received an estimate of £15,000 to undertake an extract of the CBCS from EDS from EmployeeG, a Senior Executive Officer within the IMS Business Unit. However EmployeeF, also from the IMS Business Unit, commented in his interview that the cost of such a scan is closer to £5,000.

IV.15 Clearly, concern over the cost of responding to the NAO's information needs was a key factor in determining the course of subsequent events. However, it should be noted that EmployeeD

also queried why NAO would want this information in her 5 March 2007 email, stating *"We need to be sure why NAO want this (I think it will be discussed at the meeting on 14th March) - if this is going to happen every year there may be a cost implication, unless we can use the compliance scans. Do you want someone to go to this meeting to represent you and feedback to you? (I think it's going to be much wider than compliance). Are you OK with complying to NAO's request in this instance?"* EmployeeA, in interview, stated that he took no action on the receipt of this email as he understood EmployeeD to be saying: *"this is how we are going to meet the sort of pressure from the NAO to get a cut down sample quickly by reusing what we have and the people who know how best to do that are the people at this meeting on the Wednesday."*

IV.16 It is clear that EmployeeD, in her role as secondary SPOC, took it upon herself to investigate how best to respond to this initial NAO request. One option under consideration at this stage was to allow the NAO to exploit the full CBCS scan held by CC. However, it should be noted that at this stage, no HMRC staff either envisaged or proposed that this data would be taken off-site. EmployeeF stated at interview that he had received a telephone call around 12 March 2007 from EmployeeD in which she asked about the possibility of obtaining a full extract of the CBCS records to be provided to the NAO. EmployeeF has stated that he subsequently challenged this request in a telephone call with EmployeeD and suggested, as an alternative, that NAO could select samples rather taking the entire data set. EmployeeD responded to EmployeeF in an email (copied to EmployeeA, EmployeeE, EmployeeH and EmployeeB) dated 12 March 2007 timed at 11:59am which stated:

> "*As discussed last week. NAO have requested details of all new and terminated Child Benefit cases to help them understand the sampling process. Following discussions with IMS colleagues, there has been a recent 100% scan of the Child Benefit computer system and the results have been passed to Compliance. There is a meeting this Wednesday in London with NAO auditors, EmployeeE and EmployeeH from Compliance and statisticians from KAI and National Audit Office to discuss various aspects of the Child Benefit audit. It would be helpful for NAO to have sight of an* ***example of the extract*** *to enable them to understand what the records contain. NAO are entitled to go where ever and have access to anything – without exception. They are a governing body who have absolute right to visit any part of our organisation and view any records/information we hold. As this information currently exists there are no cost implications to us in this instance, we cannot refuse them access. EmployeeA, Process Owner of Tax Credits and Child Benefit is fully aware of the current position regarding this audit and supports this request for information. Can you please arrange for one dozen cases from the 100% scan to be forwarded to EmployeeB for onward transmission to NAO as soon as possible please? Happy to discuss further."*

NAO access to information and authorisation for data removal

IV.17 EmployeeD's above email raises two points for further consideration. The first point is her incorrect assertion that the NAO has overarching powers of access to information. In fact, the Information Disclosure Guidance (IDG 65800) to HMRC staff for dealing with the NAO, as displayed on HMRC's intranet (see also Section V of this report), states that *"The NAO has a right of access to documents and materials which it reasonably requires to carry out its functions in relation to HMRC."* This is not to say that the NAO did not have good grounds for requesting this information, rather that the assumption that the NAO had unfettered and unregulated access was erroneous. Moreover, this IDG also asks that NAO provide a clear explanation as to why they require this information. In this regard, EmployeeF's challenge would appear prudent, and had his challenge been escalated to a more senior level within HMRC, the data might have been prevented from leaving its premises.

IV.18 The second point is the issue of apparent authorisation for the release of data by EmployeeA, a senior HMRC official, and more importantly precisely what was covered by this authorisation. In their respective interviews, both EmployeeD and EmployeeA remembered having a telephone conversation on this subject and recalled that EmployeeA suggested offering the NAO a sample of twelve live cases. EmployeeA has informed my team that the only authorisation he granted was for the sample of twelve cases to be provided and that he was not aware that a copy of the data download was to be given to the NAO to take off-site from WVP in either March 2007 or October 2007. EmployeeD has confirmed at interview that EmployeeA authorised the release of the twelve sample cases but she was uncertain as to whether authorisation had been granted by EmployeeA to provide the NAO with a full copy of the data to remove from WVP. My review team (who performed a forensic examination of email traffic at the relevant times) has found no further information to clarify the point but has no reason to doubt the veracity of EmployeeA's statement. Indeed, though my team has identified other HMRC officials who knew about the provision of a sample of twelve cases to the NAO (such as, for example EmployeeI, a Grade 7 official within IMS and CBCS Asset Manager), it has not identified any such officials who gave consent for, or were even aware that there was a proposal to provide a full CBCS data download to the NAO or that this download was to be taken off the WVP site by the NAO.

IV.19 Following the above email exchange, on 12 March 2007 EmployeeH sent an email to EmployeeD (copied to EmployeeE) asking if she had been refused information and seeking clarification of the details. EmployeeD then responded to EmployeeH and EmployeeE in an email which stated that EmployeeD had been informed by IMS that a *"100% system scan"* had been carried out recently for CC, adding that she had asked EmployeeF *"to get an extract for me, and following further enquiries today by EmployeeB in Washington we were told that there were "some concerns" regarding confidentiality and the need to get security clearance before any information could be handed over. Hence my email. Hope this clears things up EmployeeH and you can get me the dozen cases today for NAO Employee2"*. This email prompted EmployeeE to respond to EmployeeD and EmployeeH (copied EmployeeB), stating *"EmployeeD, this data is originally CBO data and not CB Compliance data. If NAO want this they should go to CBO Service (IMS) for this and not to CC. The fact that we may have this data is neither here nor there; it is from the source that this should be obtained. I do not know who EmployeeF is but if he is in CB Service then he was the right guy to ask in the first place. It is not just a question of "NAO can have anything", it is a question of them obtaining from the correct source. A sample of cases "new and terminated cases" is a sample to be taken from the system, and that is a service matter. It is only by chance that we may have this"*. EmployeeE's interpretation of the NAO's level of access to information is closer to that outlined in the IDG above. However, at interview EmployeeE has stated that he was involved in no further communication around this issue and that his view at the time was that the release of the sample should have come from the appropriate data owner, not CC, who were not in a position to authorise the release of such data to the NAO.

IV.20 Later on 12 March 2007 EmployeeF forwarded EmployeeD's email of 11.59am to EmployeeJ, an Executive Officer in the IMS Business Unit at HMRC, copied to EmployeeG (a Senior Executive Officer in IMS), and EmployeeK (a Higher Executive Officer in IMS). In this email, EmployeeF issued instructions for EmployeeJ to provide a sample of twelve individual cases to EmployeeB, noting his concerns over the request for the full CBCS extract and the issues that would arise if the data was ever misplaced: *"Please see the previous email from EmployeeD – I think the third paragraph is giving me a kind of hand slapping even though I have never said NAO cannot have the data. All we wanted was for NAO to realise exactly what they are asking for, i.e. "the scan data is the live records of seven million ChB customers" when they only want to look at a dozen cases from the scan. More importantly we needed to get the assurance of how they would securely handle the disc's [sic] containing the data and how they would dispose of them once they had completed their checking.*

Obviously NAO should automatically realise this confidential information has to be protected and no doubt they would do so. However, we needed something more than a verbal request to ensure we had paperwork to back up the request. Things do get mislaid and imagine the uproar if the disc's [sic] containing the ChB customer data went astray and turned up where they shouldn't – the long knives would be out. At least we would be covering ourselves by getting the right assurance. EmployeeD has now advised that they just want twelve cases from the data scan to be sent to EmployeeB for transmission to NAO. Can you arrange for twelve cases to be sent to EmployeeB urgently please".

IV.21 On 13 March 2007 at 8.20am EmployeeJ sent an email to EmployeeB (copied to EmployeeF and EmployeeL) which included two attachments (i) the URAC document (see below) for the latest data download from the CBCS, and (ii) a sample of twelve individual's records extracted from the data download. EmployeeB then forwarded this at 1.11pm to NAO Employee2, copying in EmployeeD. In this email EmployeeB states "*Please see attached extract from the Compliance sample as requested. I hope you make sense to you than us however [sic]; this is the format the extract arrived in so it will give you an idea of style for future reference. EmployeeJ has also provided the URAC document which should provide a brief explanation of the data in the extract. Best of luck!"*. As outlined in paragraph IV.1, the URAC is a standard form document used by the IMS team to request data from the CBCS which is administered by EDS. This form is typically approved by a member of the IMS team and is prepared in consultation with the HMRC Business Unit making the request for information. The URAC relating to the March 2007 Data Download detailed specific requirements as to the information to be included and specified the following security related instructions *"The samples will be sent, by secure courier on CD's containing zipped; and passwords protected download data in ASCII format to EmployeeJ (address provided)".*

NAO's request to remove sensitive data and misunderstanding as to the response

IV.22 Having reviewed the sample of twelve cases, NAO Employee2 responded to EmployeeB in an email on 13 March 2007, asking whether the amount of data to be provided for the sampling exercise could be cut down, notably by removing address, bank and parent information:

> *"Thanks for this. I have tried to understand it and put it into my testing requirements. From my review of the extract and our telephone conversation, I think it is possible to use the live data dump but need to segregate it into two files:1) Starters …2) Leavers …*
>
> *A few queries*
>
> *a) Is the above possible to do before handing it over or do we have to take the entire file with all of the data? If this is not possible, how big is the file which I assume will be zipped. I might be able to make use of the data as it stands but I will need to check. I will need to know the total number of records as a check to ensure that I have downloaded from the CD disk(s) the right number of records.*
>
> *b) I do not need address, bank or parent details in the download – are these removable to make the file smaller?*
>
> *c) Would the file have initial headings or would it be necessary insert these? It is easier with headings but this is not essential.*
>
> *d) How much lead time do I need to give if the segregation actions are possible?*
>
> *e) How much lead time do I need to give to get records out of archive?"*

IV.23 EmployeeB forwarded NAO Employee2's response to EmployeeD at 3.06pm on 13 March 2007 and EmployeeD then responded to NAO Employee2 at 3.23pm on the same day (copied to NAO Employee4 and EmployeeA) as follows:

> *"EmployeeB has passed this over to me for my views. Your original request was for 100% scan of the data, and fortunately a scan was complete earlier this year, and we have shared this with you at no additional cost to the department. I know you are meeting with Compliance and KAI colleagues on Wednesday [14 March 2007] and all your issues regarding data extracts etc should be taken up with them. I must stress we must make use of data we hold and not over burden the business by asking them to run additional data scans/filters that may incur a cost to the department. Trust this is satisfactory for now and look forward to seeing you Thursday."*

IV.24 NAO Employee2 stated, in interview, that on receipt of the above email he "*felt like he was being told 'you are getting it all or you are getting nothing'*". NAO Employee2 also noted that he misunderstood EmployeeD reference to KAI, believing that the meeting with KAI was to explain the annual survey or random review, rather than to discuss the scan extract. Moreover, NAO Employee2 did not appreciate that EmployeeD was suggesting that KAI would be able to manipulate the data in the way he requested. EmployeeD's intentions with her above email to NAO Employee2 were made clear when she forwarded EmployeeE's email of 13 March 2007 to EmployeeA later that day with the following comments: "*For information only at this stage. Thought I'd share with you EmployeeE's reply to my emails regarding the data extract. It's all been sorted now and I have copied you in to a more recent email explaining to NAO they only got the data because it had already been obtained for Claimant Compliance. If we had to run it again it would have incurred a large cost to the department. We have agreed that any information we hold needs to be put to more than one use if at all possible. I have advised NAO that they need to discuss with KAI colleagues tomorrow different ways of extracting data because EmployeeB and I aren't in a position to comment…*". Regrettably, my team has found no evidence to indicate that the provision of the CBCS scan data was actually placed on the agenda or discussed at the 14 March 2007 meeting. As a result, the more secure option of cutting down the data internally was never raised with KAI representatives. Furthermore, at no stage in the discussions did any of the parties involved consider an alternative option for data redaction using the IDEA software contained on the stand-alone computer in the locked room, which would have been suitable for undertaking such a data manipulation exercise.

IV.25 EmployeeA has stated, in interview, that he took no action on the receipt of EmployeeD's email of 13 March 2007: *"I didn't take any [action] because I didn't need to. All it said was, we've shared this 100% data set [of twelve cases] with the NAO, there is meeting tomorrow, analysts and the compliance people whose data set this is are there and they are going to talk about how to chop it down"*. When no further information was received, EmployeeA stated that he assumed that a satisfactory solution within appropriate compliance rules had been reached. We note that EmployeeA's view, that the data belonged to CC who were providing it to the NAO, differs from the view expressed above by EmployeeE, who stated that CC did not own the data and the NAO should obtain it directly from IMS. The confusion surrounding the ownership of the data, and who was responsible for providing it to the NAO, contributed to the circumstances in which the data was first permitted to leave HMRC premises in March 2007.

The removal of the discs off-site

IV.26 We note that up until this point, there had been no communications between HMRC and the NAO which indicated that the removal of the discs from WVP was under contemplation by either party. The first documented instance in which this was raised was an email from EmployeeF to EmployeeJ on 14 March 2007, in which he recounted a telephone call with EmployeeB:

"EmployeeB rang me to say thanks about sending her part of the data from the above scan. She mentioned, however, that NAO Employee2 *was visiting CBO on Thursday and he was still on about borrowing the CDs for a short while and then returning them to us. It seems this will depend on what KAI can supply him with at his meeting with them today (Wednesday). If they can do some analysis for him he will not need the CDs."* The wording in this email suggests that NAO Employee2 may have raised this issue in a previous conversation with EmployeeB.

IV.27 It should be noted that according to NAO Employee2, he travelled to WVP on 15 March 2007 with the intention of taking the discs off-site. In his interview, NAO Employee2 stated that he was aware, prior to travelling to WVP, that his computer did not have sufficient processing power to carry out the sampling work on site and he had already contacted KPMG, which was the external audit partner on the CBO audit at that time, about undertaking this task.

IV.28 I note that there remain some inconsistencies in the evidence of EmployeeD, EmployeeB, and NAO Employee2 as to the precise sequence of events between 13 and 16 March 2007, particularly with regard to who handed the discs to NAO Employee2 and who authorised them to be taken off-site. In their interviews EmployeeB and EmployeeD recalled obtaining the discs from EmployeeJ and handing the discs to NAO Employee2, though they are unclear as to the precise date. In his interview, NAO Employee2 believed that EmployeeJ handed him the discs along with a piece of paper containing access passwords.

IV.29 As regards the more important point of authorisation, in her interview EmployeeB commented that EmployeeD appeared to have authorised the release of the discs to NAO Employee2, but the issue of whether he could remove the discs from WVP was not discussed. EmployeeD, on the other hand, has stated in one of her interviews with my team that at the time she did not believe that there was any issue with the data being taken off site, explaining she was not aware of any restriction on data leaving the building and that she considered NAO Employee2 to be a "trusted source". This failure to appreciate fully the risks involved in this data going off-site via the medium of two discs in March and the failure to obtain suitable levels of authorisation from senior management set a precedent which provided a foundation for the loss of the discs in October 2007.

IV.30 The only further documented communication found by my team that related to the removal of the discs from WVP was an exchange of emails between EmployeeB and EmployeeJ on 15 and 16 March 2007. EmployeeB stated in her email on 15 March that *"NAO Employee2 will have to take the CD's away with him tomorrow as he needs somebody in NAO to break them down further. NAO Employee2 will be back in WVP next week and he has promised to guard the data with his life and bring them back safely with him next week…"*. EmployeeJ responded to EmployeeB the following day in an email dated 16 March 2007 at 8:29am stating that he *"will make every effort to hand a hard copy of the information to NAO Employee2 today"* and goes on to say, *"As for the 7th TCO disks – your* [sic] *responsible for them until they are returned!"*. It is clear from this exchange that both staff members were aware of the risks involved of the discs leaving WVP but again failed to manage those risks in an appropriate manner.

IV.31 NAO Employee2 recalled, in his interview, that he kept the discs securely at his house over the weekend following collection from WVP, and subsequently, at some point between 16 March 2007 and 20 March 2007, NAO Employee2 handed the discs to external auditors KPMG, who were assisting NAO, to enable them to select a sample for review as part of the NAO audit. NAO Employee2 could not recall whether the discs carried protective markings, but stated that he made KPMG aware of the confidential nature of the information they contained in verbal and written briefings. NAO Employee2 noted that he was provided with the samples of data that KPMG had selected as part of the process and recalls that the bank details were blanked out as part of this

process. The discs were subsequently handed to NAO Employee4 on 20 March and stored in a safe at the NAO offices in London, before being returned by NAO Employee2 to EmployeeJ on his next visit to WVP on 16 April 2007.

Summary of events leading to the March 2007 transfer

IV.32 In summary, the events giving rise to the March 2007 transfer appear to have created a precedent which allowed a similar transfer to take place in October 2007 with far less consultation. It is clear that challenges to providing the data were made by both individuals in CC and IMS, however these challenges were not properly addressed at the time. This allowed the discs to be transferred to the NAO and taken off site without the appropriate level of authorisation or adequate consideration of the security risks of releasing such a large amount of personal customer information. I consider some of the issues raised by the March 2007 sequence of events in the "Other organisational issues" later in this part of the report. However, my team would reiterate that it has identified no evidence that any HMRC staff member above Senior Executive Officer grade knew that a full copy of the data download was to be passed to the NAO for removal from WVP in March 2007.

THE OCTOBER 2007 DATA LOSS

Change of the secondary SPOC

IV.33 The events leading to the loss of the data in October 2007 were connected with the second audit of the CBO, this time for the year 2007-08. Planning for this audit began in September 2007. One of the key differences for this audit was the transfer of the role of secondary SPOC from EmployeeD to EmployeeC, another Senior Executive Officer in the Benefits and Credits team. In his interviews, EmployeeC noted that the role was only part-time, to be handled in conjunction with his other responsibilities, and he first became aware that he was being considered for the position when EmployeeM, the Grade 7 officer to whom he reported, notified him of the fact on 4 September 2007. EmployeeD explained in an email to EmployeeC, on 6 September 2007, that her main role in the previous year had been as the first point of contact for NAO Employee2, requiring her to *"manage information flows between the business and NAO and of course keep EmployeeA and EmployeeN fully informed of emerging issues"*. EmployeeC, in his interviews, explained his understanding of the role *"as putting people in touch with people they needed to be put in touch with."*

IV.34 EmployeeD made NAO Employee2 aware of these administrative changes in an email sent on the 7 September 2007, informing him that *"my colleague, EmployeeC will be your first point of contact for future audits"*. However, it appears that NAO Employee2 liaised directly with EmployeeD shortly afterwards as EmployeeC was away from the office that day. In an email on 12 September 2007, EmployeeD informed both EmployeeC and EmployeeA, copying in EmployeeM, EmployeeO (from Benefits and Credits), and EmployeeP (an Executive Officer from Benefits and Credits) that she had been contacted by NAO Employee2 earlier that day to go over plans for the 2007-08 audit of the CBO. In addition, according to an email from EmployeeD, NAO Employee2 had acknowledged that EmployeeC would be the SPOC going forward and confirmed that he would be in contact with him in the near future.

Other interactions between the NAO and HMRC

IV.35 Despite the handover of the SPOC information request role, as in the March data transfer, my team has identified that sometimes other staff within HMRC took responsibility for NAO

liaison within their Business Units. For example, in an email from EmployeeE to EmployeeQ, a Senior Officer in CC, EmployeeC and EmployeeD on 18 September 2007 at 9:51 he wrote that "*all matters relating to NAO are managed for Claimant Compliance through my work area*". EmployeeC responded to all recipients of this email on 18 September 2007 at 11:59 stating that EmployeeQ had arranged a meeting with the NAO for herself and EmployeeE on 3 October 2007 for a *"walk through of their requirements"*.

IV.36 As a result of these other interactions between the NAO and HMRC, in spite of the email exchanges above relating to the appointment of EmployeeC as the new secondary SPOC, he was not copied in to the first email relating to the NAO's use of the next CBCS scan, which was sent by EmployeeE to NAO Employee2 on 18 September 2007 at 15:22 (copied to EmployeeJ), informing him that *"the next scan of the CBCS will be taken in the 1st week in October"* and that he should contact EmployeeJ for details of how the scan might be exploited. However, I note that, in accordance with the SPOC protocol, NAO Employee2 copied in EmployeeC on his reply at 15:25 the same day to confirm that he would contact EmployeeJ in the near future. NAO Employee5, another NAO auditor, was also copied on this email. EmployeeC explained, in his interview with my team, that on receiving this email from EmployeeE he thought *"good EmployeeE has sorted this one – job done"* and hence forwarded this email onto EmployeeP on his return from leave on 1 October 2007, with the message *"as discussed"*. EmployeeC further explained that EmployeeP was assisting him with some of the *"spadework associated with the liaison role"* and the forwarded email was simply passing on information that this issue had been resolved.

IV.37 The investigation conducted by my team has determined that, though EmployeeC was involved in handling a number of other NAO requests in the ensuing period up to the loss of the CBCS data on 18 October 2007, he was unintentionally excluded from all subsequent communications regarding the CBCS scan. As a result he was not able to escalate the issue to EmployeeA, the primary SPOC, or otherwise manage this particular information request. The exclusion of the secondary SPOC from these discussions was a managerial oversight which ultimately may have contributed to the data loss.

The 2007-08 Draft Audit Approach

IV.38 NAO Employee2 and his NAO colleagues prepared a planning document entitled "Draft Audit Approach to Child Benefits 2007-08" (the "Draft Audit Approach") on 27 September 2007 which NAO Employee2 emailed to EmployeeA on 28 September 2007, copying in NAO Employee1, NAO Employee5, EmployeeC and an external auditor from PwC, who it was envisaged would assist the NAO in performing certain controls testing activities (see paragraph III.11). In this Draft Audit Approach document the NAO sets out its planned work for the 2007-08 audit of the CBO. The document makes reference to reviews that the NAO will undertake of various different sample data sets obtained by HMRC, but at no stage does it mention that the NAO would require a full extract of the CBCS data in order to perform these reviews. At interview, NAO Employee1 confirmed, in accordance with his letter to HMRC dated 9 November 2007, that the decision to sample from the whole population of Child Benefit records had not been communicated to HMRC through oversight. NAO Employee1 further noted that the data transfer should have taken place in a manner appropriate for restricted data (i.e. by hand), on the assumption that it had also been redacted of sensitive information and encrypted.

Production and encryption of the next download of CBCS data

IV.39 One of the key areas to address in analysing these events, is the process by which the CBCS scan used by CC was created, what data this scan contained, and the levels of encryption applied

to the discs onto which the scan data was transferred. As outlined above, a scan of the CBCS is ordered by IMS (on behalf of CC) every six months from EDS at Long Benton, whom my team has been informed to be the mainframe operators of the CBCS. At interview, EDS Employee1, a manager, explained that EDS habitually undertakes this download overnight once it has received a URAC document from IMS. The URAC document was drafted in late September 2007 by EmployeeJ and EmployeeL, also an Executive Officer in IMS, and approved by EmployeeK, a Higher Executive Officer in IMS. The request was sent to representatives of EDS, copied to EmployeeR among others. The URAC document specifically requests that *"The serial data to be extracted by a bespoke process and written to 100 sequential files, fields separated by commas. The data to be written initially in EBCDIC but converted to ASCII, zipped, password protected and put onto CD's which should be despatch by secure means to be agreed"* and that the data should be sent to EmployeeR of the TCO National Intelligence Team via the IMS CBCS Asset Management Team.

IV.40 My team has identified an email dated 1 October 2007 from EDS Employee2, another EDS manager, to EDS (copied to EDS Employee1), informing them that the *"6 monthly data compliance scan for Tax Credit Office is due to run…ALS will transfer the 100 files to PC & copy to CD/DVD for the end user"*. Further, in his witness statement EDS Employee1 confirmed that the "*100 files were available to be downloaded"* on 2 October 2007, adding that he downloaded half of the files onto his D drive, in a process that *"can take anything up to 24hrs",* and that the other 50 files were processed by EDS Employee2. On 3 October 2007, EDS Employee1 recalled, he zipped the files and transferred them from the D drive to the network drive adding that *"The reason for this process is so that the files are smaller and can be copied onto removable discs. They are also password protected"*. The following day, on 4 October 2007, EDS Employee1 reported that he burned the files that he and EDS Employee2 had zipped onto two Memorex CD-R recordable 700MB 80 min discs and labelled as "TCO" amongst other markings ("CBCS Discs Set A"), TCO standing for "Tax Credit Office". I conclude from this analysis that CBCS Discs Set A did indeed contain the full records of all child benefit claimants at that time.

IV.41 The URAC document issued by HMRC specified that the files should be "zipped", i.e. that WinZip software should be used to compress the files, and password protected. My team notes from its computer forensic analysis work that the version of this software used to package the data on CBCS Discs Set A, WinZip 8.1, provides only low grade encryption. In addition, according to the testimony of various witnesses, each file was password protected with the same seven digit alphanumeric password. This low level of encryption was unsuitable for the transfer of large amounts of sensitive data on a removable medium such as a compact disc.

IV.42 EmployeeJ, in his interview, recalled collecting CBCS Discs Set A from the EDS Long Benton office in person on 4 October 2007, and handing them to the CC unit on his return to WVP. EDS Employee1 sent the passwords for each disc to EmployeeJ in an email on the same day. In accordance with past practice, once received by CC, the data was uploaded on to the stand-alone computer at WVP for analysis purposes, with the original CDs being retained in the locked room.

Initial NAO request for the download of CBCS data

IV.43 There have been a number of differing accounts published relating to the production of copies of the next CBCS data scan. In the following paragraphs, I set out my understanding of these events derived from my team's various investigative activities. In summary, my team has identified that four such copies were made in the period up to the reporting of a security incident on 8 November 2007, but it was in fact the original copy CBCS Discs Set A which was ultimately mislaid.

IV.44 The first request by the NAO for CBCS scan data in the October sequence of events was a telephone call from NAO Employee2 to EmployeeJ on 2 October 2007. EmployeeJ reported at interview that NAO Employee2 asked for a copy of the full scan in this conversation and that he had responded by challenging the need for a full copy of the data. In his interview NAO Employee2 stated that he had cited the need for continuity with the March 2007 data transfer and EmployeeJ asked that he document the request via email. In the subsequent email from NAO Employee2 to EmployeeJ on the same day, copied to NAO Employee5, NAO Employee2 asked for a *"copy of the data scans being carried out in early October 2007 and early February 2008"* for NAO audit purposes and indicated that the discs should be sent to NAO Employee5 at the NAO offices in London. In his email, NAO Employee2 made reference to the previous data scan he received in March 2007 by stating that *"last time we had a 100 zipped files on 2 CDs",* emphasizing to EmployeeJ that he should ensure *"that the CDs are delivered to the NAO as safely as possible due to their content."* NAO Employee2 also requested that NAO Employee5 contact EmployeeJ by telephone once he had safely received the two CDs so that EmployeeJ could email him the passwords.

IV.45 My team observes that NAO Employee2's request for information on 2 October 2007 was sent to EmployeeJ directly and not copied to EmployeeC, the relevant SPOC. At interview, NAO Employee2 said that he had been directed to EmployeeJ as the relevant person to contact by EmployeeE's email of 18 September 2007 and he had copied EmployeeC on his response. However, my team further observes that the request was for a full scan of the data rather than an exploitation of that data as suggested by EmployeeE in his earlier email on 18 September 2007. This lack of clarity at more senior levels of HMRC as to what information was being requested by the NAO, and the non-participation of either of the SPOCs in the discussions on its provision, meant that no suitably senior official was able to make a decision on its release. The description of the need for this information as due to "continuity" from the previous audit reflects the precedent set by the March data transfer. Moreover, in his interview, NAO Employee2 explained that as his request for a redaction of some of the data had been flatly rejected in March, he felt he had no choice but to ask for a full copy of the scan.

IV.46 To compound matters, as in March, the issue of the provision of the CBCS scan data was overlooked in a subsequent meeting between some of the key parties. Notes from the above-mentioned 3 October 2007 meeting between NAO Employee2 and representatives from CC, were taken by EmployeeQ and outline the discussions around CC's workplan for the year and the NAO's interest in the random review sample. The notes do not mention any discussion of the NAO obtaining a full copy of the CBCS scan. Moreover, in her interview with my team, EmployeeQ confirmed that NAO Employee2's data request was not discussed at the meeting, nor was she aware of it at that time. The meeting was attended by NAO Employee2, EmployeeQ, EmployeeS (a Higher Executive Officer from CC at HMRC) and an external auditor from PwC (see paragraph III.11). At interview, EmployeeE explained that EmployeeS attended this meeting in his place as he was unable to do so for personal reasons and provided an email documenting this fact.

The sending of the CBCS data via untraceable internal mail

IV.47 My team notes that NAO Employee2's initial data request was not acted upon immediately. EmployeeJ forwarded NAO Employee2's first email request on 5 October 2007 to EmployeeR from CC (copying in EmployeeL and EmployeeK), requesting that he assist NAO Employee2 by arranging for a *"copy of the latest 8th scan data to be forwarded as detailed below"* . In his interview, EmployeeR explained that he did not act on this email as he was uneasy about providing the information to the NAO and did not feel that it was part of his job. He therefore did not create a copy of the discs prior to going on holiday on 12 October 2007.

IV.48 EmployeeJ stated at interview that he was not in the office for long periods between 14 and 18 October 2007, but on his return he realised that EmployeeR had not produced the copy discs as expected. He subsequently contacted EmployeeT, an Administrative Officer from CC at HMRC, and repeated the request for a copy of the full CBCS data download on two discs. EmployeeT reported at interview that he had attempted unsuccessfully to create two such discs using WinZip 8.1 and NERO software, and as a result he was forced to hand EmployeeJ the two original discs provided by EDS on 4 October 2007, i.e. CBCS Discs Set A, which as noted previously had password protection. A copy of the CBCS data remained on the computer in the locked room. My team has been able to confirm EmployeeT's version of events through its computer forensic analysis work.

IV.49 EmployeeJ stated, in his interview, that he placed the two discs in a jiffy bag with the NAO address in Buckingham Palace Road in London written on the front, and confirmed that this jiffy bag was put in a yellow "tax-post" envelope which was then placed in the 'out' tray in the IMS area at WVP. EmployeeJ has confirmed that at the time he believed this to be a secure courier service operated by TNT. Confirmation that the package was placed in the post tray was provided by EmployeeU, a Higher Executive Officer in IMS at HMRC, in her interview, in which she *"remembers EmployeeJ putting the first set in the out tray"* and *"recalls vividly seeing the yellow bags. This was unusual as there is little post and yellow bags aren't typically used"*.

IV.50 My team notes that it identified an email sent by a senior representative of TNT, after the data loss had been reported, explaining that the Tax Post system it operates is "non-documented", whereas it also operates a fully IT enabled track and trace service from the same address. Indeed, I understand that this service was later used to send the replacement discs (see below). In this email the TNT representative also explained that although the Tax Post system was an internal HMRC service, the NAO address in Buckingham Palace Road is contained within TNT's database as a government address. According to the TNT representative, the address would have been recognised as such by the TNT delivery team and the envelope would normally have been delivered there, rather than being returned to the sender in WVP.

Time pressure leads to the creation and sending of a second set of discs

IV.51 It is well-known that the set of discs posted on 18 October 2007 never arrived at their destination and, despite extensive searches by HMRC, TNT and The Metropolitan Police, they have never been found. At interview, NAO Employee2 expressed his belief that the discs had indeed first been posted on 18 October 2007, adding that on 22 October 2007 he returned to the NAO head office and searched for the discs in the post room but was unable to locate them. EmployeeJ also noted that on 23 October 2007 NAO Employee2 attempted to contact him but he was unavailable, attending an important meeting at the Long Benton site. EmployeeC stated that NAO Employee2 subsequently telephoned him, sounding "*angry (very direct and short)"* because the discs had not arrived and requiring an explanation. During this conversation, EmployeeC has stated that he explained to NAO Employee2 that he was unaware that any emails had been sent and asked him to explain both the background to the call and EmployeeJ involvement. EmployeeC added that this was the first time he was made aware that *"on 18 October two disks containing the full data downloads of CB records were posted to the NAO"*. EmployeeC was also unaware as to the content of the discs at this point. At interview, NAO Employee2 explained that there was considerable pressure to complete the audit within its designated time period, hence his assertive tone in the conversation with EmployeeC.

IV.52 Following this telephone call on 23 October 2007, EmployeeC sent two emails to EmployeeJ, the first at 09:53, copying in EmployeeP, requesting that EmployeeJ contact him

urgently to confirm that the discs had been sent. The second email was sent at 17:15, copying in EmployeeI and EmployeeP, to highlight the urgency of the situation and suggest a contingency plan, if the discs did not arrive on 24 October 2007, to prepare a set of duplicate discs and courier them to NAO Employee2 by the morning of 25 October 2007.

IV.53 On 24 October, EmployeeJ received a call from NAO Employee2 to arrange for a duplicate set of discs to be prepared and couriered to the NAO as the original discs had not arrived. NAO Employee2 recalled in his interview expressly requesting that these be sent by secure, traceable overnight post or courier. Following this telephone call, EmployeeJ approached EmployeeV, an Executive Officer in CC at HMRC and EmployeeT to obtain additional copies of the discs. According to EmployeeT, he subsequently produced two further copies of the CBCS scan discs, one as a back up copy ("CBCS Discs Set B") to be retained within the secure room, and a second copy to comply with EmployeeJ's request ("CBCS Discs Set C"). EmployeeT's recollections of his actions have been confirmed by my team's computer forensic analysis of the stand-alone computer. EmployeeT then recalled handing the discs to *"a woman in IMS"*. My team has not been able to ascertain absolutely the identity of this woman, but it may have been EmployeeK.

IV.54 In his interview, EmployeeJ remembered checking on his computer that CBCS Discs Set C were password protected, but he discovered that they were not. As a result, EmployeeJ saw that the discs were returned to CC in the secure room and a new set requested. In his interview, EmployeeT stated that the same woman from IMS returned some thirty minutes later claiming that CBCS Discs Set C were not password protected. EmployeeT said that he subsequently used Winzip 8.1 to zip and password protect the files on the hard drive of the stand-alone computer, before burning a copy on to two CDs ("CBCS Discs Set D").

IV.55 Again on the 24 October 2007, EmployeeJ recalled packaging up CBCS Discs Set D along with a memo to NAO Employee2 which noted that the discs were a copy of the CBCS scan originally sent on 18 October 2007 and requested that NAO Employee2 call upon receipt to receive the passwords. EmployeeJ stated that he had personally taken the package to the post room and that this time he sent them via registered tracked courier to NAO Employee5 at the NAO. Once the discs had been posted, EmployeeJ telephoned NAO Employee2 to inform him that CBCS Discs Set D had been sent and to look out for the original set. In addition, EmployeeJ sent an email to EmployeeC and EmployeeK, copying in EmployeeI and EmployeeU, confirming that the duplicate discs were being couriered. Finally that day, EmployeeJ informed EmployeeK via email of the passwords required for the CBCS Discs Set D. My team notes that these were not the same passwords as were used on the lost CBCS Discs Set A.

IV.56 On the morning of 25 October 2007, EmployeeK emailed NAO Employee2 to inform him of the passwords for CBCS Discs Set D. That afternoon EmployeeJ telephoned and then emailed NAO Employee2 to confirm whether the discs had been received and to express his concern over the missing set. NAO Employee2 confirmed, via email later that day, that he had received the discs and that he *"will keep a look out for the other set until Friday when it will have to be NAO Employee5."*

IV.57 In summary therefore, I conclude that there were a total of four sets of discs containing the full CBCS data produced in October 2007, as summarised in the table below:

Set	Description	Destination
A	Original discs produced by EDS on 4 October 2007	Sent to the NAO on 18 October 2007 and subsequently lost.
B	Back up discs produced by CC on 24 October 2007	Retained by CC in the secure room containing the stand-alone computer.
C	Additional set of discs produced by CC for IMS on 24 October	Returned by IMS to CC because they were not password protected. Retained in the secure room.
D	Further set of discs produced by CC for IMS on 24 October	Sent by internal recorded delivery by IMS to the NAO auditor on 24 October. Received by the NAO on 25 October.

Subsequent communication regarding missing data

IV.58 It is clear to me that the loss of the data in October and the method of its transfer prompted concern among a number of the parties involved. However, a security incident was not raised until 8 November, some 2 weeks later. On the evening of 24 October 2007, NAO Employee2 sent an email to EmployeeC, an external auditor from PwC and NAO Employee5 entitled *"Audit requests and queries"*. One of the key elements of this email was to raise the issue of the transfer of data, with reference more specifically to the next scan at the end of January 2008, between HMRC and the NAO. NAO Employee2 wrote: *"We need to work out a better way to get this data down to NAO…..Hand delivery or a better ETA? It is the uncertainty and delay which causes problems and in this case some extra costs for both parties"*. EmployeeC responded to NAO Employee2's email on the 26 October 2007, copying in an external auditor from PwC, NAO Employee5 and EmployeeP, stating that he hoped NAO Employee2 had received the scans and adding that, if necessary, to ensure they are delivered on time in the future either he or a colleague would deliver it personally.

IV.59 On the same day, EmployeeR emailed EmployeeC, copying in EmployeeQ and EmployeeS expressing his concern with the situation. He stated *"…My team recently supplied EmployeeJ with the October discs which he posted to Audit however these apparently did not arrive and new discs were copied. From a compliance point of view we have grave concerns over this sort of data being missing, I would fully endorse a 'hand to hand' transfer in the future."*

IV.60 EmployeeJ noted in interview that he contacted NAO Employee2 again on the 31 October 2007 to ask whether the original discs had arrived. NAO Employee2 reportedly confirmed that they had not been delivered however he was moving offices and therefore some post was taking two or three weeks to arrive. EmployeeI recalled in his interview that a decision had been made within IMS after discussions with EmployeeW, a Senior Executive Officer within IMS at HMRC to raise a security incident if the discs had not been received by the NAO within another 5 working days.

IV.61 On the 5 November, EmployeeJ emailed NAO Employee2 to ask whether the missing discs had been located. EmployeeJ stated, in interview, that he had attempted to contact NAO Employee2 by telephone on 7 November 2007 but could only reach his voicemail.

IV.62 Also on 7 November 2007, EmployeeU emailed EmployeeJ asking him to raise a security incident report following their discussion. EmployeeJ raised the security incident report, the following day, and confirmed this by email to EmployeeU, EmployeeK and EmployeeR. One can only speculate about what might have happened if the failure of the discs to arrive as expected on

19 October had been raised immediately with senior officials. An immediate search may have had a greater prospect of success than a search started nearly three weeks later.

Summary of events leading to the October 2007 data loss

IV.63 In summary, the events giving rise to the October 2007 loss were predicated by the custom and practice from March, though a lack of clarity in communications and failure to involve sufficiently senior HMRC staff were contributory factors in both cases. The key difference in October was the method of transfer, the Tax Post system operated by TNT, which was far less secure than hand delivery, and gave rise to the eventual loss. I consider further the issues raised by the October 2007 sequence of events in the "Other organisational issues" section later in this part of the report.

V Overview of relevant policies and procedures

INTRODUCTION

V.1 Under its terms of reference, I have been required to examine the policies and procedures in place at HMRC at the time of the loss, and review why such procedures failed to prevent the loss of confidential data, highlighting any shortcomings. This examination would be incomplete without some analysis of the accessibility of these policies to HRMC staff and the methods by which they are communicated. These issues are summarised in this section of this report. I have not provided a detailed outline of the relevant policies and procedures on the grounds that to do so could help any individual or organisation trying to circumvent them.

V.2 In addition, my team has explored whether specific HMRC policies and procedures were breached, although it should be noted that the IPCC has considered the conduct of the individuals involved. My team has identified two serious breaches of policy regarding the lack of authorisation for disclosure of the full CBCS scan and the method of its delivery via the untraceable internal mail.

V.3 As with all of its findings, my team has communicated the issues in this section to HMRC management in the course of its work. As a result, HMRC has taken remedial action to correct the policy and procedure shortcomings identified.

V.4 HMRC's security policy is principally contained in the Departmental Security Standards Manual ("DSSM") which is held on the HMRC intranet. The DSSM sets out the policy, objectives and security standards which apply to all employees handling departmental assets. My team has been told by HMRC that its security policies were structured to align with Cabinet Office inter-departmental security policy for all government departments.

V.5 In addition to the DSSM, HMRC has a series of IDG policies which provide specific direction on the circumstances in which information may be disclosed outside HMRC (notably to another government department, agency or public authority), and to other Business Units within HMRC. IDGs are held on the HMRC intranet and also published on its external website. There is a specific IDG, IDG65800, which deals with the provision of information to the NAO.

ADEQUACY, ACCESSIBILITY AND COMMUNICATION OF POLICY

Some DSSM and IDG policies lacked sufficient detail and strength to guide staff

V.6 Though HMRC policies are wide-ranging and do cover staff obligations regarding information security, some of the policies in this area were too generic at the time of the data loss incident, lacking sufficient procedural detail to guide staff in the specific circumstances. For instance, the IDG to which staff were to refer when disclosing information to external parties was insufficiently detailed to cover the events in question and it was unclear how it should have interrelated with DSSM policy. Notably, the IDG covering HMRC's disclosures to the NAO failed to offer guidance as to the removal of data from HMRC premises, the medium for transferring

information to the NAO, the existence of a SPOC for such information flows, or from whom authorisation should be sought for any such disclosure, stating only that it should be cleared "with a senior manager". I note that the IDG does state that, *"The NAO has a right of access to documents and materials which it reasonably requires to carry out its functions in relation to HMRC."* However, this statement is not found in the "Procedure to follow" section nor linked to it on the HMRC intranet.

Inadequacy of removable media and encryption policies

V.7 Arguably the most significant policy shortcoming at the time of the data loss related to removable computer media and encryption. The policies dealing specifically with removable media represented guidance for the development of policy on authorisation and documentation for removal, rather than designating actual procedures for obtaining such authority and ensuring an audit trail. Similarly, departmental policies did not require the encryption of information protectively marked as "restricted". This level of security was reserved only for higher protective markings and there was only limited guidance within DSSM policy regarding whether the aggregation of large amounts of sensitive data such as contained on the lost discs could require a higher protective marking: *"Where there is an aggregation of protectively marked information, consideration must be given as to whether the information as a whole requires a higher marking."* (DSSM3210)

V.8 It is clear to me that, following previous data losses, HMRC was aware of a specific need to strengthen its policy in relation to encryption of removable computer media immediately prior to the loss of the discs in October 2007. My team identified a document drafted by HMRC IMS entitled "HMRC Removable Computer Media Management Strategy" (version 0.2 dated 15 October 2007) which sought to require encryption for all such forms of media. Unfortunately this positioning paper had not yet been developed into policy or guidance at the time of the loss of the discs containing the child benefit data. This also raises a view expressed by several interviewees in the investigation, namely that while HMRC's operational procedures are frequently updated, it has struggled to make IT security changes required to keep pace with IT developments. The speed with which IT has developed in recent years makes it imperative that security policies are regularly reviewed to ensure that they deal with all the types of IT processes undertaken within the organisation.

Better implementation and enforcement of policy is required

V.9 As highlighted above in the case of departmental policy on removable media and encryption, the DSSM policies often contain guidance for Business Units on producing policies and guidelines, rather than specific documented processes, and those Business Units sometimes fail to grasp wholeheartedly this responsibility. The end result is that employees find no actual policy or procedure to which they can refer when the need arises. In particular, existing policy tasks each Directorate (or Business Unit) with developing and maintaining its own Security Management Systems (SMS). However, my team has found only limited evidence of such SMS having been drafted, implemented or enforced, and even then only to a moderate standard. Moreover, there appears to be only limited communication and interaction between each Directorate and the central Security and Business Continuity (S&BC) function on security issues. One of the points raised by a number of the interviewees is that such departmental "policy" is often based upon common sense and past practice rather than a formal, detailed procedure. The result is uncertainty and a lack of uniformity between Business Units in terms of procedure.

Policy could be made more accessible and better communicated

V.10 The point above leads to the question of the dissemination of policy through HMRC and its accessibility to staff. The primary dissemination method for information security policy in HMRC is via its intranet. However, almost all interviewees contacted in my team's investigations expressed a lack of knowledge as to exactly where on the intranet, security policy is to be found. In addition, staff have noted that the intranet search function is unhelpful in generating relevant results for search terms such as "DSSM".

V.11 As outlined above, whilst departmental policy envisages that policy reminders are disseminated within each Directorate from the top down, in practice, according to the interviewees, this has not occurred with any degree of frequency. Responsibility for security education, per DSSM11495, lies with line managers. Specific responsibilities of line managers are further outlined in DSSM11500 which states that they should ensure their people are aware of their security responsibilities, receive any baseline security training relevant to their role and any other specialist training as required.

V.12 The lack of accessibility to security policy and failure to deliver its messages has resulted in few HMRC staff understanding the department's policies and procedures around information security. Indeed, a large number of interviewees were completely unaware of the existence of the DSSM or the IDG and therefore the policies and guidance contained therein.

BREACHES OF POLICY AND PROCEDURE

IDG covering disclosure to the NAO

V.13 The first question to be considered in any analysis of possible procedural breaches is whether the relevant IDG covering disclosure to the NAO was followed in the data loss incident. IDG65800 is a concise document, stipulating only that an individual in HMRC who receives an information request from the NAO is required to do the following:

(a) Request that the NAO provide a clear explanation of why they want to see the documents requested; and

(b) Clear the disclosure with a senior manager.

V.14 In the March 2007 data transfer, the initial information request from the NAO was made by a telephone call from NAO Employee2 to EmployeeD so it is not possible to gauge its clarity. In her subsequent email to EmployeeA, EmployeeD acknowledges that HMRC needs to be "sure why NAO want this" information, but there is no subsequent evidence in the ensuing communications between these parties that the NAO was ever asked to clarify the rationale behind its request. Perhaps more pertinently, there is no evidence that either EmployeeB or EmployeeD sought the approval of a senior manager for the disclosure and removal off-site of the entire CBCS data set.

V.15 In the actual data loss which occurred in October 2007 my team has found that EmployeeJ did request an explanation of NAO Employee2 on 2 October, though whether he cleared the disclosure with a "senior manager" is questionable. IDG65800 is ambiguous as to the grade and Business Unit of this senior manager and does not specific what form the clearance should take. As a result, it is difficult to measure the actions of HMRC staff against it. For example, it could be contended that the original email sent by EmployeeE on 18 September, directing NAO Employee2 to liaise with EmployeeJ, provided the requisite senior manager clearance, as EmployeeE

holds a higher rank within HMRC than EmployeeJ, albeit in a different Business Unit. However, EmployeeE's email did not explicitly refer to the information being sent off-site, and referred only to the exploitation of the CBCS scan rather than the disclosure and transmittal of the entire scan itself. Even in the absence of specific wording in the relevant IDG, it is reasonable to contend that any authorisation ought to be sufficiently clear and explicit to cover the circumstances of the disclosure in question. It would therefore be difficult to argue that EmployeeE's email represented sufficient authorisation.

Appropriate authorisation

V.16 IDG65800 is not the only guidance or policy which covered authorisation requirements for data removal from HMRC premises. DSSM 5320 states that *"Equipment, information or software must not be taken off-site without appropriate authorisation."* Furthermore, under DSSM 1110 all HMRC staff must be aware of the sensitivity of all HMRC information and ensure that HMRC information is not disclosed outside HMRC unless authorised. Although these obligations are not well-defined, they would appear to have been breached in both the March and October incidents.

Method of data transfer

V.17 The other HMRC policy which appears to have been breached in October is that regarding the transfer of the data via the untraceable Tax Post system. DSSM 6720 requires Managers and Suppliers to ensure that *"reliable transport and authorised couriers are used"* and that *"any process involving the physical transportation of media has a full audit trail throughout"*. As outlined in section IV of this report, whilst EmployeeJ believed the Tax Post courier service to be secure, it was in fact a non-documented service, and therefore provided no such audit trail.

VI Other organisational issues

PEOPLE AND CULTURE

Prioritisation of operational delivery over information security

IV.1 Based on the interviews conducted, it would appear that, as a general rule, staff below the Senior Civil Service level, prioritise operational delivery over information security in the execution of their day-to-day roles. This finding is consistent with previously-mentioned lack of awareness amongst staff of the existence of security policies. Some examples of this sequence of priorities are set out below.

IV.2 Large amounts of data are transferred both within HMRC and to external government bodies with insufficient regard to risk and security. Interviewees have cited a number of such examples of data transfer:

(a) Transfer of data via unencrypted email and removable computer media. For instance, the results of analytical work performed by CC are routinely saved onto USB flash drives or CDs, transferred onto team members' computers and provided to the Benefits and Pensions team by unencrypted email. According to the interviewees, the amount of data transferred in this manner ranges from several records to several thousand records.

(b) Data scan creation similar to the CBCS scan. My team was informed that there is an exercise, similar to the creation of the CBCS scan, carried out for the Higher Education Funding Council for the purposes of statistical and trend analysis. EDS are reportedly requested to run the scan, zip the information and then return the information to HMRC. However the information is not as sensitive as the Child Benefit information and does not contain data such as bank details and addresses.

(c) Other instances of provision of large amounts of data on discs to HMRC. KAI is the main analytical service to HMRC but my team understands that it also provides this service, in some cases, to the Department for Work and Pensions (DWP). I have been made aware of at least one regular transfer of a large amount of DWP data on a CD to KAI for statistical analysis.

VI.3 As outlined above, HMRC has not always been swift to effect necessary changes to its systems with regard to information security. For example, while previous information security incidents have resulted in the delivery of recommendations to HMRC management (such as those contained within the Chilver Report), the implementation of such recommendations could have been more timely.

VI.4 Lastly, I should draw attention to the possibility that HMRC staff involved in the March data transfer could have manipulated the data to remove sensitive information such as bank details, without the need for the full data set to be transferred outside the organisation. I understand that KAI had the necessary skills and technology to undertake this task, and indeed this was suggested as a viable option but was not pursued through misunderstanding. In addition, the computer forensic analysis conducted by the review on the CC computer in the locked room identified that

it contained IDEA software suitable for undertaking such a data manipulation exercise. However, this option was overlooked.

Lack of policy awareness

VI.5 My team has uncovered a distinct lack of awareness, amongst those who have been interviewed as part of the investigation phase, of policies and personnel relating to information security. When asked specifically about whether they knew of the existence of the DSSM or IDG, the majority of interviewees responded that they had not, nor knew how to access it via the departmental intranet. Moreover, the existence of a Departmental Security Officer or the IT Security contact was also unknown to the majority of interviewees.

VI.6 Furthermore, whilst some of the interviewees referred to the "cascade" culture of dissemination of security information (i.e. from the top down), others had no knowledge of it and opined that it was an ineffective means of educating staff on information security.

Lack of training

VI.7 In line with previous findings, my team identified little training of HMRC staff in relation to information security. Some interviewees claimed that individual departments lacked sufficient budgetary resources for information security training. Others commented that there was no dedicated IT security course available to them and that any security training received at induction had been limited. Moreover, for those who had worked at HMRC for a long period of time, additional security training (as and when new legislation, such as the Data Protection Act, had come into force) did not appear to have been made available. It was also evident from the interviews conducted by my team that that the acquisition of a new role, or promotion within the organisation, would not trigger additional security training. I have found little to contradict these interviewee claims in my *Wider Review* of information security across the organisation. A compounding factor appears to be the lack of job or role descriptions for staff, which leads to confusion as to an individual's responsibilities, and the often erroneous assumption that responsibility for staff training lies with someone else.

GOVERNANCE AND ACCOUNTABILITY

Accountability for the ownership and guardianship of data

VI.8 Accountability for the ownership and guardianship of data is insufficiently defined within HMRC. This issue is particularly acute when different departments are working together.

VI.9 My team has determined that the data guardianship role has been held and debated on previous occasions within HMRC, but it had lapsed at the time of the data loss. According to HMRC documents, EmployeeX had held the data guardian role for Child Benefit in 2004, but there is no further information to indicate what the role entailed and whether it was continued after the merger of the Inland Revenue (IR) and Her Majesty's Customs and Excise (HMCE). My team has identified email communication prior to the data loss incident in which aspects of the data guardian role are debated by HMRC staff, but ultimately without resolution, and there was no such post at the time of the incident, though a data guardian has since been appointed. The lack of an appointed data guardian at the time of the incident was a significant contributory factor in the loss of the data. It is highly unlikely that the discs would have been permitted to leave HMRC premises in March without the authority of the data guardian, nor would a properly trained data guardian have permitted the use of internal post for the October transfer.

VI.10 One of the clear points emerging from the interviews is that at the time of the loss there was no consensus between Compliance, IMS and B&C as to who owns the Child Benefit Scan data. This lack of clear and defined accountability contributed to the lack of appropriate approval for the transmittal of the data scans to the NAO.

VI.11 Another contributory factor brought to my team's attention by one of the interviewees was the fact that in previous years there had been a dedicated onsite data security team at Waterview Park. That team had operated as both a contact point for all data security issues and as the responsible body for data security issues. However, this dedicated onsite data security team had reportedly been disbanded prior to the data loss incident.

Lack of clarity surrounding authority requirements

VI.12 Authority requirements and accountability for decisions relating to data transfer are neither well defined nor understood within HMRC. Staff neither sought nor believed they should have sought authority for the removal or removal method of large amounts of sensitive data from HMRC. In the March and October incidents, and more generally, authority to transfer data is sought or considered by very few interviewees. Linked to this is the confusion which arises when different departments are working together. One of the interviewees commented that most people at Waterview Park feel part of a single Child Benefit team, and as such are prepared to accept direction from senior members of other departments without seeking approval from those to whom they directly report within their own department.

VI.13 Consequently there were insufficient levels of management supervision and knowledge of events leading to the loss of the discs containing the scan data. Senior managers were unaware that the data had been removed from HMRC premises in March and October, or that such plans were envisaged by junior staff. EmployeeA, B&C process owner at HMRC was unaware that the scan was sent to the NAO in March or October until the loss incident was reported.

VI.14 It is interesting to note that when an original scan is run for CC, a URAC document must be completed. The URAC sets out the parameters of the scan (to enable EDS to produce it), but also explains in detail the rules for transfer of the scan from EDS to HMRC. Details covered include the method of transfer ("by secure courier on CD's containing zipped, and password protected download data") and the individual to whom the information should be transferred. This document reportedly requires the sign-off of two senior managers. However, when exactly the same data is copied for the purposes of a different recipient (NAO), no such senior manager sign-off appears to take place.

Relations with the NAO

VI.15 Staff involved in the discussions with the NAO in October, even those with SPOC responsibilities, took limited interest in the details of the NAO's information requirements and requests. EmployeeC of HMRC, secondary SPOC for NAO liaison in October, took little interest in the details of the information requested / supplied to the NAO at that time. Part of the problem appears to be the fact that there is no formal definition of the SPOC role, and hence those undertaking such a role are not aware of their obligations and responsibilities. There appears to be no link between SPOCs and data ownership responsibilities.

VI.16 The processes and procedures to be adopted in relation to liaison with the NAO lack clarity. In particular there is limited understanding of legal powers held by the NAO in relation to the request of information. Several Child Benefit staff believed the NAO had overriding power to request any information whatsoever. This means that even if staff were to follow the two

requirements in the relevant IDG, they would not be testing the NAO information request to see if it was information which the NAO reasonably required in order to carry out its functions in relation to HMRC.

VI.17 Lastly, certain communications from both HMRC and the NAO over the latter's information requirements for audit purposes were not sufficiently clear. The NAO did not stipulate in its audit planning documents issued to HMRC management that it would require a full CBCS scan sample in October. However, the NAO felt that it was forced to accept a full scan of the CBCS data in March because they perceived there to be no alternative. This was in part due to the misunderstanding within HMRC regarding the options available for redacting sensitive data. The circumstances for the March transfer then set a precedent for what took place in October, ultimately culminating in the data loss. In addition, the NAO did not make HMRC aware of its intention to remove the data from HMRC premises to undertake its analysis until a very late stage of the discussions, allowing little time for consideration of the risks and possible consequences.

PART 2

The Wider Review

VII *The Wider Review* – Executive summary

VII.1 Information is at the heart of everything that HMRC does. This information is often sensitive (names, addresses, details of earnings, bank details), covers almost the entire UK population and is essential for HMRC to go about its business. From birth (Child Benefit) to death (Inheritance Tax) this business touches your life. If you are employed, self-employed, a tax credit recipient, or have a national insurance number, you are a customer[1] of HMRC. All employers and businesses in the UK are customers of HMRC. When you buy a house (stamp duty), goods in a shop (VAT), goods from abroad (customs duty and/or VAT), HMRC is involved in the process. All of these processes, all of the transactions that happen around us as customers of HMRC require information – and between them, these processes and transactions annually bring in some £423bn to the Exchequer and result in some £18.5bn being paid out in Tax Credits[2].

VII.2 HMRC has undergone significant change in the past few years. Two separate departments, IR and HMCE with different systems and different cultures have been brought together into a single entity, HMRC; prior to this merger, National Insurance and Child Benefit processing was transferred from the DWP to IR; Tax Credits was added to IR's portfolio of business, introducing a very different set of demographics into the population that it serves and putting HMRC into the business of giving out as well as collecting money. And, of course, HMRC has to administer the changes enacted each year in Finance Acts. These changes individually and collectively represent good decisions which have created the platform from which to build a high quality efficient administration.

KEY FINDINGS

VII.3 Having concluded my *Wider Review* of lessons to be learnt from the loss of the two unencrypted child benefit discs, I am now firmly of the view that the incident was symptomatic of a wider problem. My findings can be summarised as follows:

- Information security, at the time of the incident, simply wasn't a management priority;
- Even had it been a priority, HMRC's organisational design and the governance and accountabilities underpinning it would have made it extremely difficult for it to be felt as such;
- Even with a more suitable organisational structure, the fragmentation and complexity that has accompanied the changes that HMRC has had to absorb makes information security difficult to control;
- HMRC's information security policies were inadequate and those that they had were unduly complex and not adequately translated into guidance or training for the junior officials who needed them;

[1] HMRC uses the word customer for those individuals or businesses with which it interacts in the administration of its various responsibilities. It thinks of itself as a business delivering services to those customers. I use these terms throughout the report in that sense.
[2] Figures are from 2006-07.

- HMRC continues to operate processes that hark back to a paper-based, rather than a digital, world; and
- Morale is low in HMRC and management needs to continue to focus on engaging with staff as the department embarks on a period of further change.

VII.4 In the main body of this part of my report I provide more detail on each of these six summary findings, however my main focus is on the future – on making recommendations that, when followed, will improve information security at HMRC. The challenge here is to make sure that my review has not fallen into the trap of making existing processes more secure when the fundamentals of the processes themselves need to be revisited. A good example comes from my key finding on fragmentation and complexity. As products have been added to HMRC's portfolio over time, little integration between them has taken place. The products effectively operate as discrete businesses, each with its own set of processes and supporting systems, but are also served by cross-cutting functions such as customer contact and debt management. Thus PAYE, National Insurance, Child Benefit and Tax Credits (to name but a few) each have their own supporting systems, each of which contains a separate customer record – meaning that the same individual customer can have four separate customer records. Maintaining these separate records is both inefficient and increases information security risk because of the constant need to bring this information together (e.g. for compliance purposes and for management information purposes). Putting better controls around the existing set of processes and supporting systems will improve information security, but to reduce information security risk to acceptable levels will require more fundamental change.

VII.5 Recognising that any change to fundamentals will take time, I have set out both specific recommendations and a longer term direction of travel. I am happy to say that HMRC has accepted all of my recommendations (and indeed has already made progress on 39 out of 45 of them, implementing 13 of them) and has endorsed the direction of travel. Throughout my review, I and my team have been continually impressed by the commitment and professionalism shown by staff and are encouraged by their overall positive response to the steps HMRC is taking.

VII.6 My review has been conducted alongside work across Government on information security, led by the Cabinet Office. The Cabinet Office project draws on our experiences, and has set out minimum measures to apply across Government, on which Departments and agencies will build according to their circumstances. I support its approach and conclusions. The recommendations in this report are consistent with them, and build on the common measures to develop an appropriate package for HMRC.

VII.7 In the short term the emphasis for HMRC needs to be on **control** - on improving controls around existing processes. The short term recommendations in my report tend to be people-orientated, for instance about training and awareness and about ensuring clarity of governance and accountability.

VII.8 In the medium term the focus moves to **consolidation**. The recommendations here have more of a process and technology flavour to them – information security levers that typically have a longer lead time to implement than those around people.

VII.9 In the longer term the direction of travel is very much towards **transformation**, moving HMRC away from its current operating model where it typically takes responsibility for collecting and maintaining data on its customers, to one where its customers, be they individuals or businesses, entrust their information to HMRC on the understanding that HMRC will keep it secure – and predominantly maintain it themselves. And to keep their information secure we advocate that HMRC joins up its islands of information, moving to a single customer record for individuals and a single customer record for businesses.

VII.10 And what, you might ask, is the connection between information security and the direction of travel? The answer is simple. The fewer islands of information you hold and maintain on your customers (and bear in mind the picture is currently highly fragmented in HMRC) the less the need for workarounds and transfers to keep data synchronised – meaning less likelihood of data loss; the more customers maintain their information, the less the need for repeated interaction with them to check details are current and the more likely it is that their data is up to date – meaning again less likelihood of data loss (less correspondence, less chance of it going to the wrong address).

VII.11 There is nothing new in such a transformation. It has been successfully embarked upon in other sectors (for example internet banking). It is also the transformation at the heart of the Government's Service Transformation Agreement ("STA") and the transformation that was underpinning HMRC's Departmental Transformation ("DTP") Programme until the programme was drastically slimmed down, losing the Integrated Customer Management ("ICM") programme – which would have, for instance, delivered a single customer account. As regrettable as the Child Benefit data loss incident was, one positive may yet flow from it. It may provide the burning platform for these transformations, recognising it as an imperative rather than a luxury.

VII.12 For HMRC, transformation has profound consequences on several fronts:

- Improved information security – fewer islands of information, less need for data transfer;
- Improved data integrity – customers are responsible for keeping their details up to date and these details are held once rather than duplicated several times;
- Improved efficiency – reduces the currently large proportion of HMRC activity that relates to correcting and maintaining customer records;
- The potential to redeploy staff to improve tax yield – the substantial effort freed up from maintaining data can be redeployed on risk-based assurance type activities, for instance on targeting those that need help to comply or those that might be tempted not to comply;
- Improved customer service – reduction in unnecessary contact; no need for customers to know the structure of HMRC to do business with it; and
- Improved staff satisfaction – more fulfilling jobs through reduction in routine error correction, and jobs that link more strongly to the purpose of HMRC.

VIII What has changed since the incident?

VIII.1 In my Interim Report, I noted that HMRC had already taken all of the immediate actions I would have recommended. I am pleased to say that HMRC has significantly reduced the risk of further data loss since the incident.

VIII.2 Key actions that HMRC has taken to achieve this include:

- Making changes to the HMRC organisational structure at Executive Committee (ExCom) level – to ensure that lines of accountability for information security (and other) matters are clear;
- Initially creating a new post Director of Data Security to drive forward immediate improvements. This has now been subsumed into the Director of Governance and Security who heads up a newly created Directorate;
- Appointing Data Guardians for every area of HMRC to act as a ready source of information and guidance;
- Increasing significantly the visibility of senior managers with front line staff. ExCom members and Directors are meeting face to face with large groups of HMRC staff across the country to explain what is being done about the data loss, how HMRC is improving information security and what HMRC is doing to recover its reputation;
- Issuing new clearer at-a-glance data security guidance, giving examples of what can be sent by what mechanism in which circumstances including a pocket rulebook, of which 111,000 have now been distributed. Every member of staff is required to discuss its content and how it will be applied/used within their team with their line manager;
- Developing and piloting a half-day mandatory Information Security Workshop. Full roll out of this will have been completed by the end July with everyone in HMRC from the Chairman down attending and having their attendance recorded. Non attendance will be tracked and followed up. HMRC is on track to have completed 95% of the roll out by the end of June;
- Re-designing and re-launching HMRC's induction training to include mandatory data security elements;
- Developing mandatory on line information security refresher training/awareness - with tests – for all staff. Once rolled out, this will need to be completed annually;
- Immediately reviewing post room processes and practice to identify high risk information security issues. The quick win recommendations from this review are now being implemented;
- Reviewing the commissioning of paper outputs to determine the minimum information required;

- Locking down write accesses to removable media drives across the whole of the HMRC IT network. Some accesses have subsequently been restored but only for business critical use and with the personal approval of the Business Unit Director and the Director of Data Security/Security & Governance;
- Banning the use of unencrypted laptops outside secure premises;
- Introducing new controls whereby all staff and managers must apply a three-step test to all potential bulk data transmissions (do the data need to be sent; if they do, get senior approval; and then make sure the data are moved with appropriate security);
- Introducing new rules for bulk data movements: via secure automated electronic routes or where this is not feasible using encryption (for disc transfers for example) or exceptionally where tape rather than disc has to be used the delivery route must be secure;
- Working on a secure electronic transfer mechanism with external partners, piloting it with banks.

IX What has *The Wider Review* found?

In my introduction, I set out six summary findings. I expand on each below.

INFORMATION SECURITY NOT A MANAGEMENT PRIORITY

IX.1 In the first half of the report I set out the narrative of how the incident came about. As can be seen from some of the email trials in that narrative, the more junior staff involved in the incident clearly voiced their concerns about handing over the data to the NAO, but were overruled by their immediate superiors – at least in part to save the cost of producing a bespoke set of data. It should be noted, though, that my team did not find any evidence of cost efficiency in the form of headcount reduction adding to information security risk. Indeed, HMRC has a 'pre-surplus' list of people whose jobs no longer exist but who continue to be on HMRC payroll and who can be deployed on overflow or backlog type work.

IX.2 We derive further evidence of information security not being a priority from observing that:

- The generic policies around information security that were issued from the centre were inadequate and tended not to be translated into Business Unit specific procedures – and no consistent assurance regime was in place to ensure that this translation was completed;
- The S&BC function which was responsible for information security policies was weak in skills and experience and commanded no authority across the business;
- HMRC did not and still does not possess documentation of its data flows at a level which would have allowed it to assess risk;
- HMRC did not employ any information security professionals at the time of the incident; and
- Staff received little or no training in information security.

IX.*3* *We say information security has to be an explicit and recognised management priority going forward.*

AN UNSUITABLE ORGANISATION DESIGN WITH MUDDLED ACCOUNTABILITIES

IX.4 The decision to merge IR and HMCE was the right one, for the reasons set out at the time, and I support it. The new management for HMRC designed the structure for the new department. At the time, heavy emphasis was placed on the need to tackle established silos within the business. Merger or no merger, at heart, HMRC is a high volume transaction processing business. In my view, such a business is best served by a traditional, hierarchical type of organisational structure. It is not suited to the so-called 'constructive friction' matrix type organisation in place at the time of the data loss. Good evidence for this comes from:

- The Director Generals, more than one of whom commented to us that they felt themselves to have no accountabilities under the organisation put in place following the merger, and all of whom agree that the new organisation gives them a much clearer focus;
- Trying to establish accountability around the incident itself: responsibility lay across five different parts of the business - Product and Process (own the policy and the design), National Processing (responsible for operations), CC (responsible for investigating and seeking to prevent fraudulent Child Benefit claims), IMS (responsible for technology) and S&BC (responsible for setting information security standards). These different parts of the business each reported into different Director Generals; and
- The data guardian role, which had only recently been implemented to combat a fundamental flaw in organisation design - the lack of data ownership. At the time of the incident, this role was still not understood.

IX.5 Following the Capability Review of HMRC conducted by the Cabinet Office and the data loss, a new organisation structure has been adopted. We think the new organisation structure is a positive step forward – but it is still emerging. Later in the report, we make recommendations to help develop it further.

IX.*6* *Information security cannot be a priority without an organisational structure and underpinning accountabilities that allow it to be such.*

FRAGMENTATION AND COMPLEXITY

IX.7 HMRC operates a hotch potch of systems some of which date back to the 1970s. These systems have been added incrementally with little attempt to integrate them and a host of workarounds, often involving data transfers, exist to keep them synchronised and to extract management information from them. This fragmentation is compounded by the highly distributed nature of HMRC. Work is also transferred, sometimes in hard copy, between these different locations, in order to manage workflow. Managing this legacy is a considerable challenge.

IX.8 Some facts that bring this to life. HMRC

- Operates some 650 different systems;
- Has a further 4500 Business Developed Applications (mostly Microsoft Excel & Access), of which 550 have been classified as business critical by Business Units;
- Operates from some 900 sites/offices;
- Sends out some 300 million items of mail a year.

IX.9 Small wonder then, that when the Director of Data Security imposed a ban on non-encrypted bulk data transfers following the data loss incident, several data transfers were uncovered that senior management in HMRC was not aware were happening, including at least three regular downloads of the entire child benefit database – the same information that was reported lost in November 2007. These were regularly downloaded onto non-encrypted media and put into internal mail.

IX.*10* *HMRC has significantly reduced the risk of further data loss since the incident. However, when there are so many islands of information and so many data transfers going on, and while simple guidance is not available to staff, further data loss nonetheless remains a distinct possibility and more needs to be done. Investment will be required to continue the reduction of risk to an acceptably low level, although the review process is identifying data transfer practices which can simply be stopped at no significant cost.*

INADEQUATE INFORMATION SECURITY POLICIES

IX.11 S&BC is responsible for setting information security policy and standards for HMRC, documenting them in the DSSM. The DSSM specifies that each directorate should have its own SMS, which is where centrally issued policies and standards should be translated into procedures that are locally applicable and relevant. However, the SMS's are of variable quality and several remain draft at the time of issuing this report.

IX.12 The DSSM is held on the HMRC intranet, runs to hundreds of pages, is not easy to navigate and is not tailored to the individual searching for guidance – meaning it is largely unused.

IX.*13* *For information security policies to be effective and understood by staff, they need to be simple, short and relevant to the business they concern.*

EMBRACING THE DIGITAL AGE

IX.14 Although the volumes have declined a little, HMRC continues to rely heavily on paper-based communications. Last year, for instance, HMRC sent out around 300 million letters and mailings to its customers, an average of 8 per household and 68 per business. The media it uses for data transfer is similarly archaic. For example, the Magnetic Media Handling operation in Longbenton, Newcastle, accepts all media (reel to reel tape, cartridges, floppy discs, CDs etc.) on which employers submit their end of year returns and could be designated a museum if the criteria were variety of media no longer generally used (media, incidentally often associated with systems incapable of creating encrypted data). Whilst part of the reason for HMRC continuing to accept such media is in response to customer demand, I strongly believe that HMRC should be stronger about which media it will and won't accept – particularly when this can drive whether or not data can be encrypted.

IX.15 As well as the media and the channels that HMRC employs, its modus operandi similarly harks backs to a pre-digital era. For instance, HMRC never seems to start from the base of the information it has. Good examples are the self-assessment process for employees where the majority of people copy their information from the P60 and P11d given them by their employer – information that HMRC already has – and Tax Credits where the application form starts from scratch although HMRC nearly always has details on that customer. Both of these examples contribute to information security risk by requiring unnecessary exchanges of data and by creating islands of information that require additional exchanges to keep them synchronised.

IX.*16* *Legislation may need to be changed so that HMRC is able to specify how its customers exchange data with it – but the incident gives a compelling reason for changes that go beyond the implementation of controls around existing processes. The changes required are consistent with the Government's transformation agenda which centres processing and data around the customer. HMRC could position itself as the leader in this field.*

MORALE IS LOW

IX.17 HMRC has gone through enormous change, including making efficiency gains and shedding staff, which naturally impacts on morale. Staff are weary of change. A clear message from the workshops we have run with frontline personnel is that the average member of staff has the impression that decisions are short term, tactical and largely cost-focused. The data loss has put further pressure on morale.

IX.18 We have observed the significant personal effort that the Acting Chairman has invested in getting around the organisation meeting and listening to staff – for instance through the 'town hall' meetings – and the warm reception he has received. These meetings have received very high feedback scores from staff.

IX.19 For the Department to move forward, HMRC needs to continue to engage with its staff in this way. Staff need the right level of understanding and engagement with what HMRC stands for and its direction of travel, the right attitudes and behaviours, and a willingness to adapt and learn new skills and ways of working. This is doubly important given that the nature of controls that can be augmented or put in place in the short term rely on the co-operation of staff. Automated controls (e.g. in systems) will take longer to implement.

IX.*20* *HMRC needs to continue to engage with its staff. The engagement of staff is a critical factor in getting information security to be seen as a priority and to be acted upon across the organisation.*

OTHER INCIDENTS ARE CONSISTENT WITH THESE FINDINGS

IX.21 As part of my *Wider Review*, the review team spent some time analysing the causes of other information security incidents within HMRC, the more significant of which had previously been brought to the attention of the Information Commissioner's Office ("ICO"). The findings from this had a high level of consistency with those articulated in this section. First, in terms of organisational design, unclear data ownership, accountability and contractual management seem to be have been key contributory factors to these other incidents. Second, in terms of people, insufficient security education and awareness hampered employees in discharging their responsibilities in respect of information security. Third, in terms of process and technology, the lack of articulation of end-to-end data flows at a level that facilitates effective risk management, together with a fragmented IT estate, also impacted negatively on the ability of the organisation to effectively identify and manage its information security risks.

X How have we gone about our work?

X.1 As far as possible within the confines of an independent review, we have sought to work jointly with HMRC and have made our recommendations as the review has progressed rather than leaving them for this final report. This has meant that HMRC has both been able to make good progress implementing our recommendations, and to ensure that their current activities are consistent with our findings. Section XV gives more details on the progress HMRC has made in this regard.

X.2 Broadly speaking, the work we have undertaken has comprised four key activities:

1. HELPING HMRC SET TARGETS FOR INFORMATION SECURITY

HMRC has now set itself clearly articulated targets that, once attained, will make it world class from the perspective of information security. The targets are based on an industry recognised standard, ISO27002, and are described in more detail in the next section.

2. ASSESSING SELECTED BUSINESS UNITS AND MAKING RECOMMENDATIONS

We selected fifteen Business Units to look at in detail, prioritising those that process large volumes of personal data and those that provide corporate services such as IT. Each of these we assessed against criteria based on ISO27002 supplemented with additional criteria from the Information Security Forum and from our knowledge and experience, chiefly around people and governance. We have been through detailed recommendations with each unit which are summarised in this report. When followed, these recommendations will move HMRC towards attaining its targets.

3. REVIEWING AN HMRC-CONDUCTED EXERCISE ANALYSING ALL OF ITS OUTPUTS

In my interim report published before Christmas, I recommended an HMRC-wide output review looking at all outputs (electronic and physical, internal and external). Given the scale of this task, I suggested that HMRC should undertake it and my team review it. This approach enabled speedy and comprehensive coverage while building buy in from those involved. The review is well underway and we have seen initial results. The focus is on eliminating unnecessary outputs, reducing the data to a minimum on those that continue to be required and, for the latter, on making sure the method of transmission is as secure as possible.

4. CREATING THIS REPORT

This report summarises at a high level the recommendations that come out of the investigation of the data loss, the wider analysis conducted in the Business Units, and the review of HMRC's outputs. In addition, it sets a long term direction for HMRC and reports on progress to date implementing the recommendations made during the course of my work. In the interests of brevity

and of security, I have not included the hundreds of detailed recommendations that have been made mostly at Business Unit level.

X.3 The Business Units my review team visited were:

- Tax Credit Office
- HR & Learning
- Knowledge Analysis and Intelligence
- Child Benefit Office
- Estate Support Services ("ESS")
- Customer Contact
- Legal and Governance
- Anti Avoidance Group
- Internal Audit
- Debt Management and Banking ("DMB")
- Pay As You Earn and Self Assessment ("PAYE")
- Information Management Services
- National Insurance
- Risk & Intelligence
- Local Compliance.

XI What does good information security look like?

THE TARGETS THAT HMRC IS SETTING FOR ITSELF

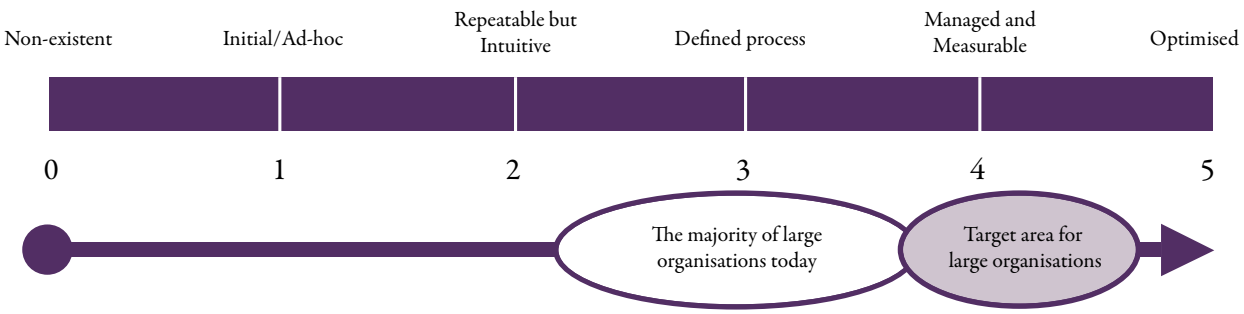
XI.1 The ISO27000 series of international standards is an increasingly used information security framework. According to the *Department of Business Enterprise and Regulatory Reform Information Security Breaches Survey 2008*, the number of organisations that have implemented the ISO27000 series is up by 60% compared with two years ago. Implementing ISO27000 strengthens an organisation's information security control processes in a structured way, though of course, effectiveness measures also need to be applied to the controls put in place.

XI.2 Organisations adopting IS027000 often assess their level of security maturity against these standards, in particular the twelve 'domains' contained in ISO27002. They use such an assessment to highlight areas of risk and to drive security improvement programmes, and typically complete the assessment by using a set of maturity statements. These statements score the effectiveness of each control using common criteria – from level 0 (non-existent) to level 5 (optimised). Using the twelve domains of ISO27002, an organisation can directly target areas where they believe that a high level of compliance and maturity would offer the greatest return. The twelve domains cover:

- Risk assessment and treatment
- Information security Policy
- Organisation of information security
- Asset management
- Human resources
- Physical and environmental
- Communication and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance.

XI.3 HMRC has completed an assessment of where it stands today vis-à-vis ISO27002 and has concluded that it lags well behind the majority of large private sector organisations, whose status is depicted in the diagram below.

ISO27002: Maturity Measurement



Rankings

0. Non-existent - Management processes are not applied at all
1. Initial - Processes are ad-hoc and disorganised
2. Repeatable - Processes follow a regular pattern
3. Defined - Processes are documented and communicated
4. Managed - Processes are monitored and measured
5. Optimised - Best practices are followed and automated

XI.4 Moving forward, the key is to set maturity targets based on the desired level of protection for key assets and the impact of control failure. Banks lead the way on this in terms of their investment in security and the level of process control maturity they wish to attain. It is worth noting that substantial time and effort is required to move beyond level 4. Few organisations achieve and sustain level 5. Typically, the cost of achieving this level outweighs the benefits gained for all but the most critical areas. HMRC is looking to assess and set key performance targets which will place it firmly in the green area. Once attained, HMRC will be the world class information security organisation its customers expect it to be.

XI.5 Importantly, banks recognise that it is unworkable to have no appetite for risk. They accept that loss will always occur and prioritise their efforts on reducing risk to an acceptable level, prioritising their controls on areas of greatest risk. The recommendations made later in this report are consistent with banking practice on information security and we would ask government to think about what the equivalent regulatory regime to that operated by the Financial Services Authority ("FSA") should be for the public sector, and whether the ICO might fulfil the role of the FSA for the public sector.

XII How to get there – the strategy

XII.1 In common with the rest of the public sector (and indeed much of the private sector), HMRC's processes have evolved over time. If the opportunity existed to design HMRC's processes from scratch, they probably would not bear much resemblance to today's. Many employees may ask why it is that they must fill out the self-assessment form when HMRC already holds much of the data required to complete it – or why the tax credit application form is blank when tax credit customer details are already held on HMRC systems – but because this is the way it has always been, few go on to question whether today's processes need to be revisited. And yet both of these examples contribute to information security risk by requiring unnecessary exchanges of data and by creating islands of information that require additional exchanges to keep them synchronised. These two sets of information (PAYE and Tax Credits), though potentially pertaining to the same customers are today stored in separate systems.

XII.2 Whilst, as a general rule, it is easier to implement something new rather than change what already exists, government cannot afford any longer not to revisit its fundamental processes and its assumptions about its relationship with its customers. To drive the changes required, I therefore set out in this section ten information security principles. I then go on to set out a direction of travel for HMRC consistent with these principles. As I mentioned in the Executive Summary, the direction of travel I am proposing is not new. It is consistent with the Target Operating Model work that HMRC has been engaged upon for some time and it is consistent with the Service Transformation Agreement. What **is** different about it, though, is the context – the loss of Child Benefit data has made information security a public interest issue. Whereas only recently HMRC's Integrated Customer Management Programme, which would have started it down this path, for instance moving to a single customer account, was dropped due to cost and payback considerations, now surely something like it must be put back on the agenda. Then it was deemed a luxury – a programme about improving the customer experience with an uncertain payback. Now it cannot be anything other than essential.

TEN PRINCIPLES FOR INFORMATION SECURITY

XII.3 Here I propose ten principles for information security in an electronic age – ten principles that could be used to underpin the service transformation agenda and which, when followed, will propel HMRC on the direction of travel we outline later in this section.

XII.4 Standards exist, of course, for controls around processes - many of our short and medium term recommendations come from applying the ISO27000 series controls. Similarly, principles exist around data protection in the Data Protection Act – but, as far as we can tell no principles exist to govern how the public sector should approach information security and what the contract should look like between it and its customers. We set out the ten principles here for HMRC but suggest that they potentially have broader public sector applicability.

1. Data about an entity (be it an individual or a business) belongs to that entity. It can be entrusted to other parties but always remains the property of the entity to which it refers;

2. It follows that it is the responsibility of the entity to maintain its own data;

3. Data becomes information when it has value. This typically happens through context and through aggregation. The ambition should be never to lose or allow undesired access to information. Key to this is segregation – i.e. separating out data when it is stored and designing jobs and the systems that support them to require a minimum of information;

4. HMRC should hold the minimum data required to perform its functions, including the retention period it holds data for. It should not, for instance hold data that it can get elsewhere but it should routinely make use of other sources of data that improves its ability to tailor its services to its customers;

5. HMRC should hold data about entities once – it should move to a single customer record for individuals and a single customer record for businesses;

6. Effective information security requires both service provider and customer to play their part. HMRC should have the powers to be able to specify secure methods of exchanging data with its customers, starting with businesses and over time including individuals;

7. HMRC should have regard to external sources of guidance on information security such as the Data Protection legislation and the guidance given to the financial services sector by the FSA.

Information security measures should be focused on the area of biggest risk, data transfer. It follows that:

8. Transfers of digital data involving physical media should be phased out completely;

9. Paper-based communications should be rationalised as to content and frequency with a long term plan of substantially eliminating them; and

10. Computers (and in the short term, any removable media) should be encrypted so that if they are lost or stolen any data or information on them cannot be accessed.

SHORT AND MEDIUM TERM: CONTROL AND CONSOLIDATION

XII.5 The levers that HMRC can pull to improve information security are strategy, people, process and technology. Good strategy in this context sets the direction of travel and makes sure that the fundamentals are right, but the best controls in the world can never ultimately eliminate the information security risk associated with the fragmented state of HMRC's IT estate and its processes.

XII.6 People, process and technology are the enablers for strategy and need to be changed and shaped over time to deliver it. In the short term these enablers can be flexed to compensate for each other. For instance, changes to technology have a longer lead time than changes to the way people use that technology, including the controls around it. HMRC will have to live with its current systems for some time and so will need to compensate for this by, for instance, bolstering the training for its staff and the procedures they must follow. Over time, as changes to technology are implemented, it will be possible to embed controls into HMRC's systems, removing the need for additional manual controls.

XII.7 Following the incident, HMRC needed to take action. As I commented in my Interim Report, it did this effectively, putting in place all the actions that I would have recommended. This was about getting on top of a crisis – about getting in control, and HMRC is still in this phase.

XII.8 The recommendations I make in section XIV of my report summarise both the *Investigation* work and the *Wider Review* work my team has performed in the fifteen Business Units they have visited. They are about control and consolidation. I have also included a small number of recommendations which, when followed, will point HMRC in the direction of travel articulated below.

LONGER TERM: A NEW DIRECTION OF TRAVEL

Control

Short-term **recommendations**: these are about getting better controls into existing processes and are a mix of business unit specific and corporate

Some cross-cutting short-term **recommendations** coming out of the Outputs Review which chart a course towards the future, increasing data security through data reduction - which also has the potential to generate savings, e.g.
- unnecessary outputs
- unecessary storage

Direction of travel - first steps centred around moving away from physical media to electronic:
- where forms storage is required
- interaction through agents
- data transfer

Consolidation

Medium **recommendations**: these are still about getting better controls into existing processes but require more time to implement (e.g. technology based recommendations or those that rub up against existing contracts in Estates).

Direction of travel - data reduction based around batching up communications by customer. Includes look at which policies/secondary legislation need to be changed.

Direction of travel - second phase of moving away from physical media to electronic:
- Agents phase 2
- Individuals
- Post to scanning/workflow

Transformation

Direction of travel - a new operating model for an electronic world.
FROM - we ask for and we maintain your data.
TO - you (plural) tell us and we keep safe (and you maintain).

A single 'account' with HMRC for individuals and a single 'account' for businesses moving away from current fragmentation.

An explicit choice of modes of operation on Trust (highly automated with risk-based assurance)/Engage (highly interactive - e.g. helping the needy) spectrum, based on the product and the customer.

A movement away from correction-based activity to risk-based assurance.

XII.9 The combination of high data-dependency, a high volume of sensitive customer data, a highly fragmented set of processes and systems, a demotivated workforce and an operating model that places responsibility for maintaining data on HMRC cannot reliably be held together only by tighter controls for long. Without more fundamental change, including a change in how staff approach information security, the risk of significant data loss remains high. This change will require an investment and a sustainable shift in behaviour. In the short term HMRC needs staff to operate in a disciplined and responsive way to the additional controls being put in place. In the longer term, it needs to rely on staff who can intelligently apply their understanding of information security to the changing needs of the organisation, using modern integrated systems.

SETTING THE FOUNDATIONS NOW

XII.10 In the short and medium term, HMRC can start laying the foundations for the new direction of travel on two fronts: moving away from physical media to electronic transfer and reducing the volume of interaction it has with its customers.

XII.11 The diagram below sums this up. The direction of travel is represented in the steps within the dotted line and shows that even in the short and medium term, when the focus is about control and consolidation, progress can be made towards transformation. This is described in more detail below.

XII.12 Specifically, in the short term we recommend that HMRC investigates:

- Ceasing to hold paper records in storage, digitising them instead;
- Banning data transfer by physical media; and
- Commencing communicating with its customers via email rather than paper. For this first phase we suggest it concentrates on agents – all of whom are capable of transacting electronically.

XII.13 And in the medium term, we recommend that HMRC investigates:

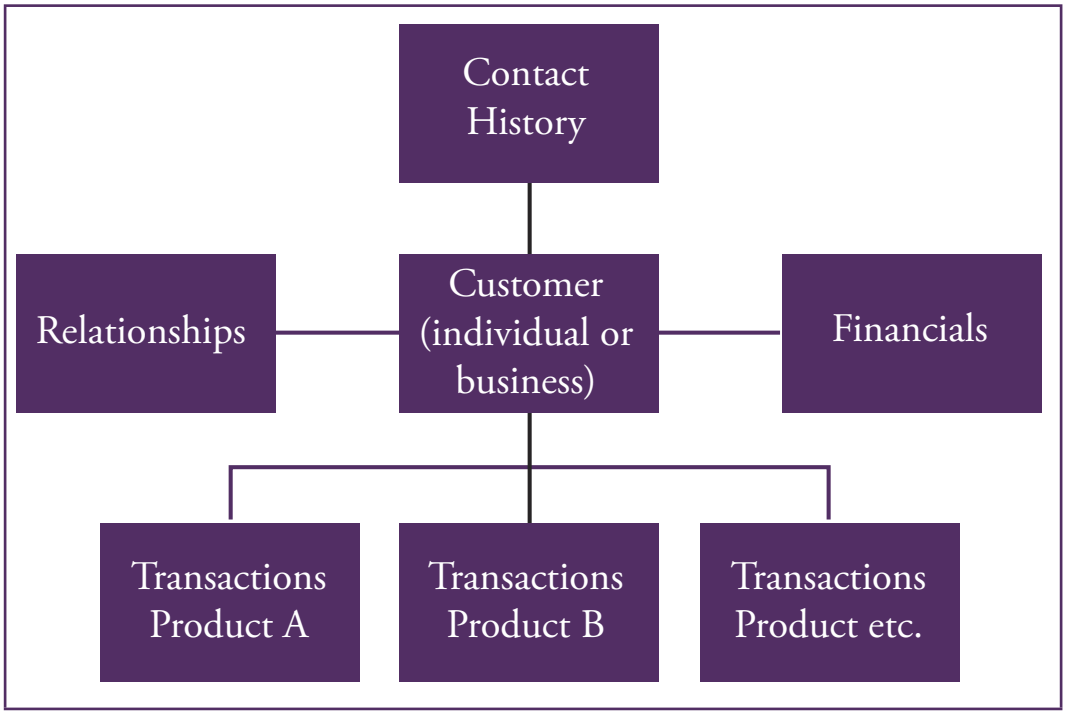
- Continuing to move away from communicating with its customers via paper – recruiting more agents to email and starting to recruit individual tax payers too, recognising that not all such customers will have access to email;
- Scanning all of its incoming post and distributing it via workflow; and
- Batching up its communications by customer (rather than each product having its own communication), reviewing and revising any policies or secondary legislation that might impede this.

XII.14 In section XIV, we recommend that these short and medium term initiatives be investigated further.

Moving to a single customer record

XII.15 HMRC's products (or 'heads of duty' as they are known) today typically operate discretely, each with its own set of customer information and financial information. Thus, the Child Benefit system holds a different customer record from the Tax Credits system and a different record from the PAYE system… and so it goes on. Each system has the potential to hold conflicting information (e.g. addresses) and contains information that is potentially of use to other systems – the read across between Child Benefit and Child Tax Credits being a particularly obvious example. The effort to keep all this information synchronised and to make information available that is useful beyond its immediate system boundary results in large volumes of data exchange, often via physical media rather than automated interfaces.

XII.16 We suggest that HMRC moves towards a single customer record model along the lines depicted in the diagram below.



XII.17 The key features of this model are:

- A separation of customer from product and other data. The benefits here are two fold:
  - Products share a common view of the customer. Rather than each product having its own version of customer details with its own processes for keeping it up to date (and the cost and effort this entails), the products would be linked to a single view of the customer.
  - In line with the principle of data becoming information when it has value, as far as possible data is stored as data, coming together to create information when needed for processing. Thus nothing other than a key to customer information would be held in the transaction details associated with a particular product. The transaction details themselves would be merely data - without using the key to link them to the customer, they would be meaningless.
- The ability to create and maintain relationships between customers. Some of HMRC's products are individual based and others rely on knowing relationships between them.
- The ability to assemble all relevant information by customer. When each product has its own version of customer details, getting a view across the customer is challenging. Such fragmentation makes identity fraud easier too with customers able to exploit the lack of centralised control over customer records to create bogus ones or to avoid detection. Assembling information by customer is also a key enabler for closing the tax gap. It will help identify those in need of help and education to comply (unintentional non-compliers) and those requiring intervention to make sure they comply (intentional non-compliers).

YOU TELL US

XII.18 I mentioned earlier the common reaction for a PAYE customer filling out the self-assessment form – why I am filling this out when HMRC has all the information I am about to send it already? HMRC's current business model assumes that it is the responsibility of HMRC to keep track of its customers, to check the information it has is correct, rather than relying on the customers themselves to keep HMRC informed. A good example of this is the movements service where some 6,000 staff are responsible for keeping track of PAYE customers as they move from one job to the next.

XII.19 Many large organisations, including my own, have moved to a self-service model for much of their HR administration, making employees responsible for maintaining their own records. Typically, this has resulted in significant savings and in better quality data – after all it is in the interests of the employee to maintain their bank details when that is their vehicle for payment. This is the sort of model we believe that HMRC should adopt – and it is a model successfully used for instance in internet banking. We believe that every HMRC customer – individual or business – should have an 'account' with HMRC that it is their responsibility to maintain. We contend that this will be popular with customers (HMRC's own customer research shows that most customers' satisfaction is inversely proportional to the amount of interaction they have with HMRC), will save money (less time spent maintaining data) and will improve information security and integrity (less customer interaction, better currency of data). It does, however, need to recognise differing customer needs – those that require 'engagement' – and have a robust assurance regime wrapped around it.

'TRUST' AND 'ENGAGEMENT'

XII.20 The majority of HMRC's customers trust HMRC with their tax affairs. They do not particularly wish to get involved in the intricacies of tax calculations – they would far rather trust HMRC to do it on their behalf. What this group appreciates the most is automation – not having to deal with HMRC or dealing with them very little. However there is a significant minority for whom the opposite is true. These tend to be customers who are needy – for instance some tax credit recipients – or those whose tax affairs are complex. These groups need engagement – involved interaction – rather than automation. The new operating model that will result from following the direction of travel must recognise this explicitly and should try to segment its customers along these lines, recognising the information security implications. Customers requiring engagement are likely to have more sensitive information stored about them and will require more interaction.

FROM CORRECTION TO ASSURANCE

XII.21 Freeing up resource from data correction activities creates the opportunity to invest more in assurance. At the moment, HMRC's mode of operation is based on all customers' data being maintained. We propose moving towards a model where the need for HMRC maintenance is risk-based, based on a customer's propensity to get it wrong (in which case they need targeted intervention). Of the total tax liability that could be collected by HMRC, some flows in automatically, some requires intervention and the rest constitutes the 'tax gap'. Estimates of the size of the tax gap vary – but it is sizeable. For instance, the official figures for the indirect tax gap published each year put the VAT tax gap at 14.2% for 2006-07.[3] Moving staff away from correction activity into assurance activities would enable HMRC to concentrate more effort into interventions that would drive up yield and drive down the tax gap.

[3] *Measuring Indirect Tax Losses - 2007*, HM Revenue and Customs, October 2007

XIII Moving in the right direction – HMRC's new organisational structure

XIII.1 The comments I made in my *Interim Report* on the organisation structure of HMRC in place at the time of the incident were consistent with those in the *Capability Review of HMRC*:

> On starting this review, my immediate impression of HMRC was one of complexity, both in terms of its many constituent parts and its matrix management structure. In particular I found it difficult to relate roles and responsibilities amongst senior management to accountability.

XIII.2 Since then HMRC has implemented a simpler management structure under which each Director-General is accountable for a defined business area. The new structure includes four main Lines of Business and a corporate centre that consists of a range of corporate functions such as human resources, finance and IT. Three of the Lines of Business are defined by a particular customer segment with which each deals, i.e. individuals, businesses, and benefits and credits recipients, while the fourth is a crosscutting Line of Business, focused on decreasing the tax gap. The roles of HMRC's existing Business Units, and their relationships with the senior management, are being redefined as a result of this restructuring.

XIII.3 At the same time the membership of ExCom, HMRC's management board, will undergo significant change as a result of the appointments of a new Non-Executive Chairman and Chief Executive, and the retirements and completion of the short-term appointments of others. All but three current ExCom members are either serving in an "acting" capacity or are due to depart by the end of 2008. The new senior management team's approach to defining the relationships between the corporate centre and the Lines of Business and individual Business Units will be important in determining their ability to influence the Department's performance on information security.

XIII.4 I believe that there are opportunities for HMRC's corporate centre to make a significant contribution to improvements in information security by advising and assisting the Chief Executive in reviewing and responding to Lines of Businesses performance on information security, and by providing superior expertise in information security to support the Lines of Business in consistently implementing good practices across the Department as a whole. In order to take advantage of this opportunity the corporate centre must acquire stronger, specialist capacity expertise in information security specifically, and in risk management in general. These specialists must combine insight into the operational issues and constraints that HMRC's managers face so that they can intervene and provide advice in ways that are practical and genuinely value-adding. The success of these specialists in making the required contributions will depend on ExCom members providing well-informed and active sponsorship of their work.

XIV What are we recommending?

XIV.1 This section summarises my recommendations from both *The Wider Review* and *The Investigation* under the headings of Strategy, People, Process and Technology. Section XV lists each recommendation and specifies whether or not HMRC has made progress on it.

STRATEGY

R1 *The role of information security as a corporate objective should be acknowledged by HMRC and work should immediately begin to formalise this objective within its mission and strategy(s).*

As we noted in our findings, information security simply wasn't a priority at the time of the incident. Moving forward, HMRC needs explicitly to make it one of its top priorities by making it a specific objective that is cascaded from the top down through the organisation and which is measured. Specifically, we recommend:

- Information security should be added as an objective into HMRC's Departmental Objectives;
- The objective must recognise balance – information security cannot be the objective to the exclusion of all else; and
- Achievement against the objective must be measured. HMRC is setting itself information security targets using ISO27002 (see section XI). We suggest these could be used as the basis for measurement – and might also give HMRC a structured way of responding to the Cabinet Office's requirement for an annual information security report.

R2 *Line of Business objectives for information security should be set to support the overall achievement of information security corporate objectives.*

For information security to be a priority throughout the business, the Departmental Objective must be translated from a corporate-wide objective into meaningful and measurable Line of Business and Business Unit objectives.

R3 *HMRC's Business and IT Strategy should be updated to make them consistent with the direction of travel set out in this report.*

HMRC's target operating models are already broadly consistent with the direction of travel set out in this report but are set too far in the future (2017) to be able to drive immediate change. We recommend that HMRC sets out in detail the road map towards a direction of travel, outlining what the business and its supporting IT will look like year by year.

R4 *HMRC should initiate a review of any policies or legislation that might need to be changed if it is to be able to specify the manner in which its customers should interact with it.*

This recommendation should be performed in conjunction with updating the Business Strategy (R3). We suggest that HMRC takes the lead on this initiative, presenting proposals for the changes it believes are required to Her Majesty's Treasury ("HMT"). The legislation might cover both businesses and individuals.

It is our view that the burden on customers of complying with data exchange requirements need not be onerous. A good example is the interfaces that HMRC has with banks (for instance to obtain interest earned details for inclusion in PAYE assessment). Based on my review team's soundings, banks would welcome HMRC specifying a secure mechanism of data exchange.

R5 *HMRC should initiate an exercise to formalise its information security strategy, making sure it supports its updated Business and IT Strategy.*

HMRC has various initiatives and standards around information security but does not have a information security strategy that articulates its goals, and how it intends to achieve them. We recommend that S&BC set out an information security strategy that can be used to drive HMRC's Data Security Programme. The strategy should include:

- Information security objectives;
- HMRC's risk appetite, in particular those critical risks that HMRC must mitigate;
- Timescales (short, medium and long);
- Measures of success;
- Key responsibilities and accountabilities, including information security governance;
- Integration within HMRC as a whole, including how the strategy is adopted; and
- Approach for ensuring compliance.

R6 *HMRC should identify 'quick wins' to set it off on the right direction of travel.*

We noted three potential quick wins in section XII, all of which we recommend that HMRC investigate further. They are put forward as candidates, are by no means comprehensive and may transpire to be more complex than at first sight. HMRC should therefore look to identify others. The Outputs Review, for instance, should be a rich source of opportunity to reduce the volume of data that HMRC transfers around internally and externally, as should the mapping of data flows recommended at R32. The key here is for HMRC to find tangible and implementable initiatives to set it off in the right direction that staff can see and get behind. The candidates recommended for consideration are:

- Ceasing to hold paper records in storage, digitising them instead. Our preference, of course, would be to minimise storage, but we do understand that in some cases, copies of records must be kept for some time. Where this is the case, we recommend

that HMRC evaluate the option to image such records and hold them electronically rather than holding them physically;

- Banning the use of physical media for moving information within and without HMRC (with the exception of creating backup tapes). Given that the vast majority of data losses occur during such transfer, we recommend that HMRC urgently puts together a plan that eliminates data transfer via physical media. This change should include the elimination of routine paper based internal communications in favour of email.

- Migrating customers away from paper-based to email-based communication. In the first instance, we suggest that HMRC looks at agents, who as businesses will all have email capabilities and can be relied on to use and check email regularly. An email is less likely to go to the wrong address than a letter and email differs from post in several key respects that make it more secure:

  - It cuts out the middle man, i.e. whoever is delivering it;

  - Sensitive files can be password protected; and

  - Receipt can be monitored.

R7 *HMRC should identify and investigate initiatives which will take it further along the new direction of travel in the medium term.*

Again, the following initiatives are given as candidates - we recommend that HMRC investigate:

- Continuing on the path of moving away from communicating with its customer via paper – recruiting more agents to email-based communication and starting to recruit individual tax payers too – recognising that not all such customers will have access to email;

- Scanning all of its incoming post and distributing it via workflow, building on the experiences of the private sector; and

- Batching up its communications by customer (rather than each product having its own communication) and potentially by household for individuals.

R8 *HMRC should seek to achieve a better balance between strategic and tactical investment.*

The business case for the direction of travel proposed in this report is potentially highly attractive but has a payback over several years. In the interim, HMRC will need to continue to deliver the efficiencies demanded through the spending review process. For HMRC to be able to break out of its current state of fragmentation and move towards the new direction of travel, it will be necessary to better align and balance investment to address both short term pressures and the longer term transformation. For instance, although HMRC has a target operating model that is consistent with the direction of travel set out in this report, its DTP does not have a project to bring together its customer records and move away from its current islands of information. The ICM Programme which HMRC had embarked upon was abandoned because of its predicted cost and because it did not meet the requirement to generate savings in the short term.

R9 *The HMRC Data Security Programme should start to coordinate and manage current security activities and initiatives as a coordinated, integrated body of work.*

HMRC has established a Data Security Programme. To date its focus has been on marshalling the various different initiatives around information security that HMRC has underway. This is entirely understandable. The initial focus of the programme was on establishing control through rapid action. The programme now needs to change its focus towards setting future direction. It should do this through an integrated programme plan where it is clear what it is the role of the centre to do and what is down to individual Business Units. This plan should incorporate the recommendations in this report as well as the recommendations coming out of the Chilver and Taylor Reports, Cabinet Office Guidance and the Outputs Review.

R10 *The Data Security Programme Board should be sponsored by an ExCom member and have members who are senior enough to ensure effective coordination and implementation.*

Conflicts between the Data Security Programme and HMRC's operational priorities are inevitable. The Data Security Programme Board must include members with sufficient seniority and insight into the full range of HMRC's activities to specify a cohesive and effective programme and to ensure its implementation in practice. It should be sponsored by the ExCom member designated as HMRC's Senior Information Risk Officer ("SIRO").

R11 *HMRC should appoint a Chief Risk Officer.*

As noted by the Capability Review, HMRC does not currently have an adequate focus on risk management. We recommend the appointment of a dedicated Chief Risk Officer ("CRO") at a Director level, under whom there would be three teams, one covering risk more broadly, one specifically covering security (both physical and information security) and one responsible for governance.

We recommend that the CRO report to the Chief Finance Officer ("CFO") and that the criteria for the appointment of any future CFO specifically include a track record of risk management experience and expertise (as is the case with the incumbent). The CFO should be designated as the Department's SIRO, in line with the requirement defined by the Cabinet Office that every Department should identify a Board member as its SIRO. HMRC may wish to make the CRO a standing invitee to ExCom meetings to emphasise the importance of the role and to enhance the CRO's authority and influence.

R12 *HMRC should appoint a Chief Information Security Officer (CISO) at senior level, reporting to the CRO.*

HMRC lacks deep professional expertise in information security at senior level. The corporate centre has an opportunity to establish strong, professional information security capability, which could be used to support - and to provide guidance and challenge to – all the Lines of Business.

The success of the information security function is dependent on active sponsorship by an ExCom member. This would be provided by the CFO who, along with the CRO and CISO would have responsibility for meeting the Cabinet Office's requirement that all Departments should "lead and foster a culture that values, protects and uses information for the public good". Within HMRC, the CISO will lead S&BC.

R13 *HMRC should establish a professional risk management function, whose roles should include supporting the Lines of Business in managing their risks through a common, Department-wide process, and supporting the CRO, the CFO and other ExCom members in the identification and assessment of strategic risks.*

HMRC currently lacks deep professional expertise in risk management, and the capacity in Corporate Governance currently consists of less than two full-time posts. Its processes for managing risks are highly dependent on a bottom-up process whereby risks are identified, assessed and escalated from within the Business Units, and the time devoted to discussion of risks at ExCom level is limited.

The risk management function would ideally include risk management professionals with substantial risk management experience in an operational environment. Its roles would include:

- Defining corporate policies, procedures and criteria for the identification, acceptance, assessment and control of risks across the Department;
- Assisting the CRO, the CFO and other ExCom members in identifying strategic risks at a Departmental level and advising them on the assessment and treatment of those risks;
- Advising the Chairman, Chief Executive and Chief Operating Officer of HMRC, and the senior management of the Lines of Business, on the risk management performance of the Lines of Business, including their compliance with agreed risk management policies, procedures and criteria; and
- Leading cultural change across the Department towards active management of strategic and operational risks, including the professional use of risk registers to support a systematic approach to risk management.

R14 *The Chairman, Chief Executive and Chief Operating Officer and their senior advisers should use periodic meetings with the Directors-General of Lines of Business and their senior management teams as a forum to support and challenge the Lines of Business on information security.*

HMRC is operating (or plans to operate) new processes through which the Chief Executive (currently the executive Chairman) will exert influence on the performance of the Lines of Business. This will provide an opportunity for the Chief Executive and the Chief Executive's senior advisers to provide support and exert pressure on Line of Business Directors-General for their performance, *inter alia*, on information security. The CFO, CRO and the CISO should support the Chief Executive in operating these processes in order to use them effectively to exert influence on the performance of the Lines of Business on information security. However, HMRC's current plans do not include regular performance review meetings between the Chief Executive and the Chief Executive's advisers with the Director-General and senior management team of each Line of Business on an individual basis (i.e. on a Line of Business by Line of Business basis, as opposed to meeting collectively). I believe that such a performance review meeting would enhance the Chief Executive's ability to exert the necessary influence on the performance of Lines of Business in relation to information security.

PEOPLE

R15 *HMRC should engage its staff by communicating the direction of travel. This communication needs to recognise how far removed from today's reality this will seem and be alive to staff perception that HMRC's priorities constantly change and that this may therefore be initially viewed with a degree of scepticism.*

There are numerous disparate activities and change programmes taking place across HMRC, adding to a general confusion about what 'One HMRC' represents, where the organisation is heading, and what this means for staff and other stakeholders.

Reported levels of staff engagement are low, driven down by a number of factors including the response of the press to the data loss incident and a perceived state of constant cost-focussed change activity.

The data loss incident could provide the catalyst for HMRC to launch a compelling vision for the future; pulling the organisation together, helping staff to understand their part in achieving that vision, and encouraging new levels of engagement. More immediately, staff need to be re-engaged if the necessary controls, which rely on their cooperation, are to be put in place.

In the short term we recommend that HMRC:

- Be honest about where it is now and clearly articulate *one* big picture of where it is aiming to be in five years' time;
- Outline the route map for getting there; what life will look like along the way, what will change and how things might look for staff and other stakeholders;
- Give staff the opportunity to contribute their thoughts and ideas on how best to reach the destination; and
- Consider ways to celebrate successes about information security moving forward.

R16 *HMRC should commence the alignment of HR, Communications, Learning and change activities to ensure that information security policies and processes are embedded into day-to-day working life and behaviours.*

We have observed a lack of effective coordination in the delivery of information security messages. This has contributed to the general level of confusion about how to apply this guidance at a local level. Feedback from workshops is that recent communications about information security have been applied differently across the organisation. Staff have received mixed messages – on the one hand being told to conform to certain rules when, on the other hand, the infrastructure isn't in place to support them to do so (for example being told to comply with a strict clear desk policy when there is no lockable storage available). We understand that HMRC is considering moving to a model whereby the Communications Business Partners within a Line of Business report to a Senior Communications Business Partner. This mirrors the approach being taken for HR and should help to embed a consistency of approach and accountability across the Communications function.

At the same time, there are a number of networks (including Comms, HR, Finance, Data Guardians, and Pacesetter) which do not seem to connect in a way that facilitates a coherent framework and approach to addressing strategic issues, such as information security, across the organisation.

To help to embed information security into day-to-day working life and behaviours HMRC should:

- Leverage existing networks, agree specific responsibilities and ensure that all related initiatives are properly co-ordinated in order to ensure:
  - A comprehensive understanding of different stakeholder needs;
  - That messages are delivered consistently across the organisation - or are tailored appropriately;
  - That the appropriate levels of information are being delivered by the right people; and
  - Links are made across the Lines of Business in order to support the sense of 'One HMRC'.
- Consider how to better join-up these respective communities to share best practice and collective learning, and realise efficiencies of scale.

R17 *HMRC should ensure that staff, at all levels, understand their responsibilities and accountabilities for information security and apply information security policies and principles in their day-to-day roles.*

Since the incident, staff have a greater awareness of the importance of information security however, confusion remains about individual responsibilities and accountabilities for information security. Prior to the incident information security was neither an explicit part of HMRC's Ambition, nor a strategic objective at the local Business Unit level; as a result, information security hasn't been referenced in role profiles (bar a few specialist roles) and has not featured routinely in the Performance Development Evaluation ("PDE") process.

To date, the organisation cannot be sure of the effectiveness of the information security messages and communications; whether they are understood, that they are reaching people via the right channels, or that they are leading to a demonstrable change in attitudes or behaviours.

These issues can be addressed as follows:

- Provide the wider context for the zero tolerance message and clarify and communicate the consequences and disciplinary process for breaches and non-compliance;
- Directors General and Business Unit Directors should work with the Data Security Programme, Data Guardians, Process Owners and S&BC to develop clear and consistent responsibilities and accountabilities for information security;
- Review, amend and formally document the role and responsibilities of the Data Guardian;
- Define each employee's responsibilities in regard to information security; making it clear where their responsibilities end and when, where and from whom they should seek guidance. Communicate these responsibilities and, where appropriate, incorporate into role profiles;
- Review all information security policies and procedures; ensure that they are up to date, make sense to the lay person, are readily accessible and, where appropriate,

tailored for the purposes of the end user. This may mean distilling key messages or instructions; and

- Agree appropriate Key Performance Indicators at Department and Business Unit level and put in place appropriate management reporting processes at all levels.

R18 *Information security messages and controls should be incorporated into all employee life-cycle processes, from attraction and recruitment through to exit.*

There are a number of opportunities though the main life-cycle events to introduce and re-enforce information security messages. In the main these are not exploited by HMRC policy or local practices.

With the exception of a small number of specific information security related roles, information security messages do not feature in the recruitment process. Whilst Criminal Record Bureau ("CRB") checks are being built into the pre-employment process for all appointments, there remain weaknesses in the local application of this process, with instances cited of staff starting employment prior to the completion of pre-employment checks.

At induction stage, guidance about information security is referenced on the HMRC intranet and an e-learning based process is supposed to be used across HMRC, however there is considerable variation in the consistency with which this process is followed. There is also a heavy reliance on the line manager to conduct induction in accordance with the policies set out by HR centrally. Records of completion of induction are held locally, if at all, and at present no routine assessment is made of how well the induction has been understood. When staff transfer between roles, they seldom receive any meaningful induction into the new role.

It is therefore difficult to have any real confidence that staff will come through recruitment and initial induction with an appropriate understanding of the importance of information security, or of what is expected of them in relation to information security in their specific roles.

Additionally, compliance with information security policy in relation to specific roles is not consistently reflected in the PDE leaving performance largely unmeasured. The disciplinary process is not explicit about the consequences of information security breaches, whether malicious or negligent.

These issues can be addressed as follows:

- Assure the completion of pre-employment checks work for both permanent, temporary and contract staff prior to them commencing work;
- Be explicit about the importance of information security in the recruitment process and about information security responsibilities in the letter of appointment and contract of employment;
- Ensure staff are aware of what constitutes a breach, the consequences, and the potential outcomes of disciplinary action;
- Mandate information security to be included as part of the induction and internal transfer process and test the inductee's understanding in relation to Business Unit and role-specific aspects;
- Do not allow completion of the induction process until the required standard is reached;

- Use local content and a range of channels for the induction process (rather than a one-size-fits-all approach), ensuring it is engaging for staff and increases the effectiveness of application; and
- Make Corporate Shared Service Directorate (CSSD), Business Unit HR Business Partners, ESS and IMS work together to develop and implement appropriate compliance checks around the exit and transfer processes in relation to system access and return of data assets.

R19 *HMRC should develop and implement a information security awareness programme that includes regular refresher training to remind and update staff of the risks and of their responsibilities.*

Prior to the data loss incident the Department did incorporate aspects of information security in its e-induction course for new starters, although the emphasis was on directing the inductee to end policy rather than making information specific to the inductee. There was no subsequent refresher training. Since the data loss incident the Department has taken a number of steps to raise awareness of the risks in relation to information security, and to clarify responsibilities and accountabilities in this respect. Some examples include:

- The release of the 'Golden Rules' and Data Security Booklet;
- The roll out of a half-day training session to all staff (currently underway); and
- The design of a computer-based data security training package to be added to the core induction for all new starters.

However, the strengthening of information security in large complex organisations is a constant challenge and requires ongoing and sophisticated efforts to raise and maintain awareness. HMRC is at an early stage on its journey in this respect. Multiple channels of communication need to be used, of which this type of training is only one.

Best practice emerging from other large organisations indicates that tailored, face-to-face training targeted at areas of high risk, combined with perhaps a generic computer-based training package for all, is the most effective and cost efficient way ensure regular refresher training (ENISA 2007).

My review team ran a workshop for the Data Security Programme team in February, highlighting the latest thinking on raising awareness of information security, and presenting how other organisations keep staff updated through mandatory annual computer-based compliance training, or similar. We are delighted to learn that HMRC is in discussion with an expert consultancy in this field to seek advice and assistance. In the mean time we recommend that:

- The CISO should develop a information security awareness raising programme in consultation with Communications and Marketing and Learning, which covers and consolidates induction training and annual refresher training;
- Face-to-face training is targeted at risk areas highlighted in risk management process;
- Induction and refresher training is made mandatory for all, is relevant to staff's day-to-day jobs, and includes testing for understanding; and
- The Learning Management System (LMS) is used to track the take-up of mandatory refresher courses and that this information be used to actively manage compliance via the performance management process.

R20 *HMRC should build appropriate levels of capability in the management of information security across the Department.*

When specialist roles or functions are created HMRC has, in the past, tended to appoint from within. Where specific experience or expertise is required in a given role there is a risk that the appointee will not have the appropriate skills or training for the role. No one we met in key information security-related posts had specialist expertise or experience. This was true amongst those we met in S&BC, in the Data Security Programme, and among Data Guardians. Whilst these individuals may learn fast, the urgency with which the Department must move to improve security means they will need to import external information security expertise.

We recommended that the Department appoint a CISO to report to the CRO, together with an information security professional for each Line of Business. This is the minimum requirement, and plans are required to ensure information security capability is developed and maintained over time. To this end we additionally recommend the following:

- Expert advice is sought on the design of the role profiles (i.e. job descriptions) and selection processes;
- As the leader of S&BC, the CISO works with HR and Learning and the Heads of Lines of Business to agree current and future skills requirements in relation to information security at all levels;
- Existing information security roles, structure and governance are reviewed to ensure the needs of the Department are met now, and in the future; and
- The CISO works with HR and Learning to put in place a robust recruitment and training process to ensure that HMRC maintains an appropriate level of expertise in this area over time.

For management assurance around information security, and for the direct line management of staff, HMRC places considerable accountability with the line management structure. However, the evidence we have from our meetings and from the workshops we ran, shows that HMRC often falls short of providing line managers with the tools, training and/or support to deliver against these accountabilities.

Our observations around recruitment, induction and the management of staff performance in particular, are that these processes are inconsistently applied. This situation is a consequence of widely varying levels of skills and experience of line managers, and the inconsistent levels of support provided to them. This has a direct impact on information security as delivery of messages, implementation of controls and levels of compliance are not consistently managed.

It is also contingent on managers to control the quality of output from their teams through effective recruitment, performance management, and management assurance around key processes and controls. Management capability will indirectly, and in some cases directly, impact levels of compliance with information security.

Guidance on these key management processes is typically provided via the intranet and basic management development training has been a casualty of constraints on investment in Learning across the Department. The use of alternative funds, secured through the Pacesetter programme, to address this gap has led to a number of local management development programmes being developed outside the control and governance of the Learning team.

We therefore recommend that:

- HMRC refreshes existing management development programmes and materials and implements a Department-wide programme that includes modules covering the core areas of information security, recruitment, induction, managing performance, managing discipline and grievance and management assurance; and
- The PDE process should be used to ensure that all line managers are clear on what is expected in terms of standards of performance in these areas, to assess current levels of capability, and to plan and manage on-going development.

R21 *HMRC should consider using Pacesetter as the means of driving changes in behaviour around information security.*

The Department has invested heavily in the Pacesetter Programme and we have been impressed with what we have seen of the Programme in both processing and 'considerative' work areas. These sentiments are echoed by the Central Programme Office and by those actively engaged in LEAN and other Pacesetter activity at the front-line.

In our view, Pacesetter principles, methods and tools could play a key role in entrenching information security controls across the organisation. From discussions with members of the central programme team, central and local Pacesetter facilitators, front-line managers and staff in the National Insurance Contributions Office ("NICO") and CBO, the collective view appears to be that Pacesetter can contribute in the following areas:

- **'LEAN' processes**: Although the 'leaning' of processes is primarily designed to improve workflow and efficiency, it can and should also be used to identify risks (such as information security) and to incorporate controls in written operating procedures;
- **Staff engagement**: Staff we spoke to in NICO and CBO reported improved engagement levels, since Pacesetter encourages staff contribution and staff are able to apply their job-related knowledge to improve processes. A number of practical suggestions from this group form part of our recommendations below. Similarly we were told that Pacesetter work in Charities Assets and Residencies (a 'considerative' work area) had helped build a sense of teamwork and shared goals, and Debt Management and Banking is currently considering the use of problem solving events to tackle information security problems;
- **Customer focus**: Whilst, to date, the focus of the Pacesetter principle of 'Customer Focus' has been directed to making it easier for the customer to pay their taxes (or receive benefits and credits), HMRC should consider extending this principle to highlight the importance of keeping taxpayers' personal data safe; and
- **Leadership**: Managers at all levels need to know how to assure information security in their work areas. Lean Academies provide training along with a robust and flexible set of tools and mechanisms (such as the workplace assessment) which could be used to support managers in assuring information security.

As described earlier, there is a significant volume of inter-related activity underway around information security. We would argue that Pacesetter, as a change programme with some successes under its belt, could be used as a central vehicle for coordinating this activity. This would require certain changes to the Pacesetter Programme as it currently operates and warrants further discussion.

More immediately, and with the support of the Corporate Pacesetter Programme, in Business Units where processes have already been 'Leaned' leadership should explore the following:

- Use of the Lean workplace assessment process for clear desk and disposal of confidential waste;
- Use of the wider location assessments as a peer review of information security;
- Flagging information security risks in work procedures (e.g. process steps for the transfer of data);
- Developing written procedures for data transfers;
- Involving the Data Guardian in the review of work procedures;
- Adding information security as a standing agenda item at weekly performance meetings; and
- Adding information security as a checkpoint prior to implementation of the Lean 8 stage problem solving process.

This will also help ensure that where Pacesetter is being used for other purposes, due consideration is given to information security. We have seen instances where processes that had been 'leaned' through Pacesetter presented an information security threat – for example the creation of 'buffers' of files of sensitive information left out over night so that they could be worked on immediately by teams coming in the morning. HMRC should check back through all processes that have been 'leaned' to ensure that none have been done so at the expense of information security.

PROCESS

R22 *Information security guidance should be simplified, shortened and made more accessible.*

The DSSM is made available to staff via the intranet. It runs to hundreds of pages, is not easy to navigate and not tailored to the individual searching for guidance. On accessing the DSSM, it is not possible to see the full contents list, different DSSMs share the same title and related DSSMs are not automatically linked – making it next to unusable.

We recommend that:

- Clear and unambiguous guidance be provided for employees in the short-term, detailing actions and steps to be followed in respect of identified, high-priority information security risk areas;
- Specifically, guidance on the secure disposal of records on electronic media needs to be updated and issued;
- The DSSM and the SMSs be simplified, assembled on the basis of principles rather than rules, encouraging the application of common sense rather than trying to account for every eventuality, backed up by a stronger assurance regime;
- The presentation of the DSSM on HMRC's intranet be improved to make it more navigable and easier for the user to access the information relevant to them. This might include tailoring the view provided to the user of the DSSM based on their access profile;

- HMRC upgrade their intranet to log which users are accessing which pages and to allow users to give feedback.

R23 *Central guidance on information security policy and standards from S&BC should be translated by all Business Units into locally applicable procedures and the accountabilities between S&BC and the Lines of Business made clear.*

S&BC is responsible for setting information security policy and standards, translating Cabinet Office guidance to make it applicable to HMRC. This is set out the DSSM which is held on the HMRC intranet. The DSSM specifies that each directorate should have its own SMS. The SMS is where the corporate policies and standards in the DSSM should be translated into locally applicable procedures. This translation is not performed consistently – the SMSs are of variable quality, and several are still draft. This needs to be tightened going forward. Specifically, each Business Unit should update their SMS in line with DSSM11235 and DSSM11240. For the avoidance of doubt:

- Accountability for setting standards and policing that these standards have been translated into locally applicable procedures rests with S&BC
- Operational accountability – accountability for ensuring that procedures are followed during the course of day to day business – rests with the Lines of Business.

R25 sets out in more detail how we recommend that the assurance regime for information security be structured.

R24 *HMRC should enhance its S&BC capabilities to take a more proactive stance on incident management.*

S&BC needs to enhance its capabilities to be able to act as an early warning system and to be able to take preventative measures. Key actions it should take include:

- A greater emphasis on analysis of trends in and root causes of incidents across HMRC;
- Estimating the cost impact of incidents across HMRC; and
- Horizon scanning of potential future threats – be they electronic or people related (e.g. organised gangs placing plants into contact centres).

R25 *HMRC should adopt a structured approach to assuring and auditing performance in relation to information security, based on the unambiguous accountability of Directors for information security within their areas of management control; assurance and audit activity carried out on behalf of Line of Business Directors-General; and corporate assurance and audit activity undertaken by the CISO and the CISO's staff.*

There is no consistent approach taken to checking that each Business Unit has translated the DSSM into a locally applicable SMS and that this SMS is adhered to. It is clear that S&BC needs to strengthen its role around checking that the standards it issues are indeed translated into a workable SMS within Business Units, as stated in R22. What is less clear is how HMRC coordinates its assurance regime to check compliance with the SMS. At the moment, this is done through a

combination of Director Assurance Teams, Data Guardians, Internal Audit and S&BC itself.

Going forward, we recommend that:

- Operational line managers of HMRC's Business Units be accountable for information security within their Business Units and implement systems of management checks in order to maintain confidence in standards of compliance and to underscore the priority attached to information security;
- The senior management of Lines of Business, including their Directors-General, Management Board sponsors of information security and their proposed, professional information security advisers, have access to resources to examine aspects of these systems and to undertake audits of practice in identified areas of information security risk. An efficient way of providing the necessary resources could be to establish capacity under the CISO to conduct assurance and audit activities commissioned by Line of Business management; and
- The CISO provide assurance to ExCom that the Lines of Business are complying with the Department's policies and procedures through a programme of risk-based assurance and audit activities. The CISO should liaise with the Head of Internal Audit to ensure that these information security-related activities are coordinated with the activities of Internal Audit. The CISO's team should have the primary role in conducting audits of compliance with information security policies and procedures, and should make resources available to assist Internal Audit as required.

R26 *Each Line of Business should identify an information security sponsor on its Management Board and should appoint an information security professional to provide leadership for information security across the Line of Business.*

The new Lines of Business provide more effective organisational units within which to manage information security, because (excluding Compliance) they encompass a greater proportion of the information flows that need to be safeguarded. We recommend strong leadership for information security within each Line of Business, involving sponsorship at Line of Business Management Board level with an information security professional reporting direct to the relevant Management Board member.

R27 *Each Line of Business should identify an appropriate risk management sponsor on its Management Board and should appoint a risk management professional to provide leadership for risk management.*

Full-time positions dedicated to risk management, supported by Management Board level sponsors, are necessary to engender the necessary degree of change in the risk management cultures of the Lines of Business.

R28 *HMRC should ensure that the mechanisms that it provides for managing key linkages between interdependent functions, for example those between the Business Units and shared resources such as Customer Contact, DMB, IMS and ESS, are effective.*

The new Lines of Business constitute organisational units that are more process-complete than the

individual Business Units. Significant hand-offs nevertheless remain that need to be managed and it is at these hand-off points where information security risk can be the highest, particularly if data ownership is not clearly established across the hand-off. HMRC plans to establish "operations level agreements" between Lines of Business and their internal service providers, and to establish various bodies such as the Performance Committee to help govern these internal customer-contractor relationships. These mechanisms are complex to manage, however, and significant management attention from Lines of Business will be required in order to make these mechanisms for managing the linkages with service providers effective.

There are in principle three generic approaches to managing these types of organisational linkages:

- HMRC has until recently based its approach on the first of these, i.e. informal collaboration between separate Business Units based on shared objectives and values. We have observed management behaviours in HMRC that focus far more sharply on fulfilling the specific responsibilities of the individual Business Unit managed than on managing linkages with other Business Units upon which the successful operation of the Department's processes depends. These behaviours are inconsistent with this first approach and would need to change before it could be adopted with confidence as a means of managing key linkages.

- The second approach, which is more formal and structured, though less flexible, is internal contracting through service (or operations) level agreements. We recommend that HMRC should, at least for the time being, adopt this more formal approach for managing linkages that are critical for the Department's success, such as those between Lines of Business and Customer Contact, DMB, IMS and ESS referred to above. We further recommend that such operations level agreements explicitly address data ownership.

- The third approach, which is both the strongest and most flexible, is incorporation of the related functions within a single hierarchical structure so that coordination can be achieved through direct supervision. We believe that this is the most effective approach where there are no overriding benefits of scale that centralisation of activities and resources in a shared service would provide. Adoption of this approach would involve more radical organisational restructuring, including the breaking up of some current Business Units such as Customer Contact and DMB, which the Department has decided not to undertake at least until the new chairman and chief executive are appointed. More radical organisational change along these lines should be considered.

R29 *The Data Guardian, and any professional information security role at the Line of Business level, should include explicit responsibility for the people-related aspects of information security.*

Assuming that R26 is implemented, each Line of Business will appoint an information security professional to provide advice and to exercise delegated authority to make decisions about information security regarding the Line of Business as a whole. As far as the Business Units within the Lines of Business are concerned, their line management has unambiguous accountability for all aspects of information security delegated to it by the Director General of its owning Line of Business. Each Business Unit has appointed a Data Guardian as the principal adviser on information security to the Business Unit's senior management team. As things stand, the Data

Guardian may have delegated authority to make certain decisions regarding information security in the Business Unit, for example in relation to the methods to be used for bulk data transfers. People management issues are central to information security.

Good information security in practice depends in part on appropriate information security policies, procedures and rules. It also depends on people being aware of those policies, procedures and rules, and having the knowledge, skills and motivation to apply them effectively. We recommend that the Data Guardian role be augmented to include advising and assisting the senior management of the Business Unit on the people aspects of information security. The Data Guardian would normally work collaboratively with the Business Unit's HR & Learning Business Partner in performing these aspects of the role. The people management aspects of the Data Guardian's role could include, for example, specifying the learning and development requirements of staff members and their supervisors in relation to information security, and advising on how information security should be taken into account in the Business Unit's approach to applying HMRC's people management systems, such as those supporting Performance Development Evaluation and discipline. Once appointed, we recommend that the information security professionals have oversight of the Data Guardians within their Lines of Business.

R30 *Each Line of Business should in the short term have a clear point of accountability for the security of mail handling, including the handling of mail by post-rooms owned by both ESS and itself.*

One of the major sources of risk to information security in HMRC is paper-based data transfers. HMRC's organisation design must therefore enable it to pay sufficient management attention to this major source of information security risk.

ESS has in hand a project with the objective of creating larger, more efficient post-rooms, which use advanced technology and common processes. We understand, however, that resources to take this project forward are limited. Furthermore there is some concern among senior operational line managers that the transfer of ownership of post-rooms to ESS would present them with problems in meeting target turnaround times for their operations.

As a short-term measure to manage the information security risks posed by mail handling we recommend that each Line of Business should place accountability for the security of mail handling on behalf of the Line of Business with one of its senior managers. This role would include obtaining assurances in relation to the operation of post-rooms operated by both the Business Units within the Line of Business and by ESS on the Line of Business's behalf. In the longer term, we believe that HMRC should make a strategic move to eliminate the need for most of the data flows that require mail handling in favour of e-mail, digitising the paper-based mail that continues to flow in, distributing it within HMRC using workflow.

We understand that HMRC has recently taken the decision to place accountability for post handling with a single Director General, This accountability will include setting standards, defining metrics, reviewing processes and driving volume reduction. It should also help coordinate existing initiatives such as the ESS project mentioned above. We welcome this decision.

R31 *HMRC should make its access control consistent across all of its systems and estate.*

Access control is not performed consistently across HMRC and should be tightened. During the course of our review we came across numerous examples of system and building access rights not

being revoked on exit or transfer and saw little evidence of an effective assurance regime. We recommend that:

- Each Business Unit should regularly review the roles and allocation of entitlements to its systems and buildings to ensure that they are appropriate. The results of these reviews should be documented and anomalies addressed;
- Regular reviews and recertification of system privileges to all systems should also be conducted at least annually to ensure current requirement and applicability to an individual's role. These reviews should be signed off by the individual and their manager(s) and the recertifications should be properly documented and stored appropriately; and
- HMRC should assess the current working model for systems access provisioning, and, in accordance with good practice, ensure that this activity is completed by the most appropriate part of HMRC – likely to be a combination of IMS (rather than ESS) and the business units for local application access.

R32 *Each Business Unit should conduct a capacity review for paper storage to determine its future requirements so that it can be compliant with the clear desk policy.*

A clear desk policy is in operation across HMRC and is being enforced with some rigour. However, in several Business Units, there is not sufficient storage for papers to be locked away, and this is frustrating staff because they are unable to comply with the policy. We recommend that each Business Unit:

- Perform a 'weeding' exercise of the documents it has stored to create capacity. This exercise should be repeated on a regular basis;
- Review what it normally stores to determine whether it is all necessary;
- Determine what capacity it is likely to require to be able to comply with the clear desk policy;
- Submit a request for additional storage, where necessary, to ESS; and
- In the meantime communicate with its staff the course of action taken.

R33 *HMRC should map its end to end data flows at the right level of detail to enable effective information security risk identification and management.*

Data flows in HMRC tend to documented at either a very high or a very low level and cannot be easily pieced together to create an end-to-end view. This makes risk assessment difficult: the greatest likelihood of data loss comes at interface points where data passes across boundaries. The blanket ban imposed by the Director of Data Security immediately following the incident on non-encrypted data transfer unearthed data flows that HMRC senior management was not aware were taking place. We therefore recommend that:

- Data flows should be identified, analysed and mapped on an 'end-to-end' basis;
- The flows should be mapped at the right level of detail to enable effective information security risk identification and management;

- Mapping should clearly follow data flows across organisation boundaries (both internal and external); and
- Once the flows have been mapped, each Business Unit should reassess and document its risks, including information security, based on the flows, identifying those that can be addressed through system functionality, either preventative or detective, and those that require manual controls to be designed and implemented.

R34 *Service level agreements should be agreed to ensure that the service meets the operational needs of the business.*

All of HMRC's existing Service Level Agreements should be reviewed and enhanced as necessary to make sure they support HMRC's information security requirements. Service levels with other government departments, in particular DWP, should be formalised and policed. This includes the development of appropriate procedures and policies to control access to networks and network resources within external networks, allowing HMRC to police its borders. These policies and procedures should be coordinated with access control policies and information exchange policies. In developing these policies, IMS should consider the differentiation between Government Secure Internet and other network connections. IMS should communicate and agree these policies with service providers, and monitor the implementation of and adherence to these procedures.

R35 *HMRC should initiate a programme of Third Party Assurance in respect of information security requirements.*

HMRC has insufficient knowledge and oversight over its third parties' compliance with information security requirements. It should urgently address this through a programme of assurance via Internal Audit, or if they do not have the capacity via an independent third party. This should start with third parties who handle post, confidential waste, off-site storage and who provide security services and move on to HMRC's IT suppliers, IMS assisting Internal Audit as required.

TECHNOLOGY

R36 *IMS should enhance the current approach to project approval for new IT systems to ensure that business owners understand the risks they are being asked to accept.*

HMRC uses the Risk Management Accreditation Document Set ("RMADS") process to assess and accredit its systems from an Information Security Assurance perspective. IMS should ensure that business owners have the means knowingly to accept the risks documented in RMADS, for example through provision of a clear business interpretation of technical risks. In addition, IMS should work with Governance and Security to develop and implement clear criteria for the acceptance of risk in information systems as part of the RMADS process. These should be sufficiently detailed to allow a structured and uniform approach to risk acceptance, they should be in line with the overall objectives of the Business Unit, comply with all relevant legal and regulatory requirements and be signed off by at least two senior managers who will subsequently own the accepted risk. Where a Business Unit wishes to accept a risk determined as Red or Amber, a detailed business case should also be produced and a time limit should be placed on the agreed mitigating actions.

R37 *IMS should review the ASPIRE contract to determine whether it reflects adequate information security.*

IMS should check the ASPIRE contract against the standards set by S&BC, and identify any terms that need to be upgraded, for instance around data transfer.

R38 *HMRC should urgently draw up its strategy for the replacement of Child Benefit systems and the transfer of the contract for Child Benefit IT Provision across from DWP.*

The main Child Benefit system, CBCS is approaching the end of its practical working life. HMRC has assessed that the CBCS remains stable and capable of continuing to support delivery of Child Benefit in the meantime, and they have started to explore strategic options for a replacement system. There is no longer full system documentation to support the CBCS (lost over the many years it has been in operation) and maintenance of the system is reliant on the accumulated knowledge of the EDS development team that supports it. This is a particular risk given the small population of developers with knowledge of the workings of the CBCS. Current estimates put the timeframe for replacement of the CBCS at a minimum of three and a half years. This situation is exacerbated by the fact that the EDS contract for CBCS and other Child Benefit systems resides with DWP under the TREDSS contract – meaning that HMRC has had little direct contractual influence over its supplier, a situation that HMRC has begun to remedy.

HMRC should urgently determine its replacement strategy for CBCS, including its data migration strategy. Given that Child Benefit is a relatively simple benefit (flat rate) and should therefore not require a complex system, HMRC should investigate whether any of its existing assets might be adapted to handle it rather than starting from scratch. This would have the advantage of sharing a customer record – and removing an island of information.

R39 *HMRC should move to an IT investment model that includes more of an emphasis on risk quantification.*

IMS should consider adopting methods for valuing risks in financial terms in order to enable the relative priority of investments designed to control risk and other investments designed to achieve direct financial benefits to be assessed with greater transparency. Such prioritisation clearly will need to be considered against other HMRC imperatives including those driven by policy.

R40 *HMRC should strengthen business requirement specification, particularly around non-functional requirements.*

The responsibility for non-functional requirements specification within the current systems development process is ambiguous. This can lead to the situation where the Business Unit specifying the change believes it needs to specify only the business-specific requirements for a project (that with which they are most familiar) and that IMS will pick up the non-functional requirements, like disaster recovery, compliance with data protection or data retention and disposal requirements. However, IMS is not always able to specify these requirements, which may be more business-specific than Business Units realise. In several cases, this has resulted in non-functional requirements remaining unspecified and the development of information systems that are without disaster recovery provisions.

R41 *HMRC should enhance its business continuity management.*

We observed inconsistent levels of completion and approval of business continuity documentation. The business continuity planning documentation which Business Units are required to maintain should be enhanced to cover information security considerations, including clearly specifying activation criteria. Similarly, disaster recovery provisions are not consistent across HMRC's IT estate and in some instances are non-existent. We recommend the following:

- IMS should assist S&BC in developing a formal policy requiring the inclusion of disaster recovery provisions in key information systems across the HMRC estate;
- On the basis of the results of the 25AW[4] project, IMS should work with Business Units to secure central funding to bring all key information systems into line with accreditation requirements, including formal disaster recovery provisions;
- IMS should set a target date for all key systems having appropriate disaster recovery provisions;
- IMS should work with Business Units to develop a formal schedule for disaster recovery testing covering all key information systems. This schedule should be implemented, and regularly updated as new systems acquire disaster recovery capabilities;
- IMS should work with Business Units and ASPIRE to ensure that disaster recovery requirements are included by default in both business and technical specifications for new or significantly updated systems. As an assurance activity, IMS should sign off on the removal of all disaster recovery provisions from business requirements, where this is requested by the business;
- A formal link between the risks held in the IMS Strategic Risk Register and the IT Services Continuity Plan should be established;
- IMS should ensure that regular reviews of business continuity and disaster recovery plans are undertaken and documented.

R42 *HMRC should continue to move the emphasis from Business Unit commissioning of IT projects to corporate prioritisation of IT projects.*

There are currently two primary sources of funding for IT projects, firstly through project business cases made by separate Business Units and secondly through IT projects commissioned by the DTP.

The funding through business cases made by separate Business Units results in a series of budgets for the improvement of each relevant system, each with its own priority based on local Business Unit issues. The Departmental Transformation Programme funds IT projects that affect the way HMRC operates, which tend to have broader IT implications. The DTP is relatively new and has started to engage in portfolio management, prioritising projects across HMRC.

However, where a Business Unit proposes a change to a shared system, they must pay for the impact of that change across all users of the system. This captures the cross-Business Unit costs but not any resultant cross-Business Unit benefits, which effectively rules out all but the most minor

[4] The RMADS process has been mandatory for new systems and major enhancements since August 2006 meaning that the majority of HMRC's legacy systems have not been assessed and accredited using it. The 25AW project is looking at 36 key legacy systems using RMADS and is being conducted through ASPIRE.

changes. As a result shared infrastructure (like Frameworks) is remarkably stagnant. This represents both a lost opportunity for HMRC to take advantage of the benefits of shared infrastructure, and, unless fixed, will be an active barrier to taking the new direction of travel forward. To move away from islands of information towards a single account for its customers, HMRC must think and act more corporately on its commissioning of IT projects.

RECOMMENDATIONS TO EMBARK ON A NEW DIRECTION OF TRAVEL

XIV.2 I have set out a new direction of travel for HMRC which is described in Section XII. This direction of travel recognises that merely to augment controls around HMRC's existing processes will not sufficiently reduce information security risk, especially given the fragmented nature of HMRC's IT estate, and that a more fundamental change is needed. The direction of travel improves information security by reducing the islands of information HMRC currently holds and by reducing the need for data transfer. It has wider benefits too, not the least of which is improved data integrity, which I articulate at paragraph VII.11. I am pleased to say that HMRC endorses the direction of travel.

XIV.3 Embarking on this direction of travel is a significant undertaking and my remaining recommendations are focused on this – on building the business case for the programme (R43) and on strengthening HMRC's internal capabilities to drive and manage it through to successful implementation (R45). In the short term, this is likely to require some external expertise (R44).

R43 *Build the business case for the new direction of travel including determining the route map to get there, the timescales, and the level of investment required.*

Following the direction of travel will require investment, investment that has not been forthcoming in the past – partly due to lack of money, partly due to planning horizons and partly due to the lack of a well-articulated business case. The business case from the perspective of savings generated *can be* attractive. We believe the steps to build it would include:

- Quantifying how many records there are by customer (individual and business)
- Quantifying how many systems support them and what the total systems cost is for this
- Quantifying how much effort goes into maintaining these records. This assessment would include all processes that have to do with change of circumstance
- Determining what legislation would be impacted by HMRC moving to the 'you tell us' operating model – for instance the ability of HMRC to be able to specify how customers must interact with it
- Determining the degree to which records, their supporting systems, the processes to maintain them and the people that operate these processes can be streamlined.

We recommend that HMRC, rather than being solely savings-driven in its business case, should also evaluate the opportunity to redeploy staff towards yield improving compliance activities – building the business case based on yield improvement rather than staff reduction.

Finally from a cost perspective, HMRC needs to determine what incremental steps can be taken to build towards the direction of travel (the route map) and the investment associated with each.

R44 *In the short term, HMRC should engage professional help to flesh out the new direction of travel, the business case behind it and the route map to get to it.*

HMRC currently lacks resource and expertise consistently to specify what it requires from its IT provider. Often the IT provider itself is heavily involved in the specification process. We recommend that HMRC engages a third party trusted adviser to help determine the most cost effective solutions and how incrementally to build towards them. We suggest that a good principle for this third party to adopt would be to always seek to re-use existing assets where possible. This would make delivery safer (the assets being reused are already proven), sooner (reduced lead time for development) and cheaper (less development required). A candidate for further exploitation here is the Modernising PAYE Processing for Customers 3 ("MPPC3") Programme which is bringing together NI and Tax Processing. This could be the first step towards having a single customer record for individuals.

Longer term, HMRC should enhance its own capabilities so that it can reduce its reliance on third parties. This is covered in R45.

R45 *HMRC should enhance the capabilities of IMS so that it is able to drive ASPIRE to deliver the enabling IT that underpins the direction of travel.*

There is a high degree of variation in the skills and expertise of IMS managers. This means they are not consistently effective in their intelligent customer role. There is also insufficient knowledge within IMS of the IT assets that HMRC (and indeed other departments such as DWP) has at its disposal, leading to a tendency to assume that any new policy requires a new system rather than looking at which existing systems might be enhanced to deliver it. This, of course, exacerbates the problem of fragmentation.

To address these issues, we propose:

- IMS should clearly restate its purpose, vision and delivery model, articulating what IMS is going to do, what it is not going to do, and its approach to maximising value from the ASPIRE partnership in terms of value for money and service delivery to Business Units. We understand that in the past three months, HMRC has commenced a value for money study to determine how its IT outsourcing arrangements can better support the business' long term requirements. Findings are due to be reported back to the HMRC Board in June 2008.
- IMS should review and re-design its organisation structure, better to align it with the delivery model implied by the purpose and vision. The design should, as a minimum, make explicit proposals about how IMS will:
    - Build up its capabilities in particular around information security, strategy & architecture leadership, contract and performance management, and risk management. We envisage that, in the short term, IMS will need to recruit to build up its professional expertise in all these areas. It may be necessary here for HMRC to make allowances for local departures from Departmental norms around reward, career management, working location and working culture where there is a need to attract and retain scarce specialist professionals;
    - Allow for clearer accountability of IMS managers for key aspects of the delivery model, consistent with the changes to line of business and corporate services accountabilities currently underway; and

- Improve HMRC's ability to co-ordinate investment, development and standards across its business, including prioritising IT investment and determining the specifications for new IT infrastructure, better to mediate between local Business Unit priorities and Departmental needs for consistent approaches to business continuity, disaster recovery and information security.

• IMS should conduct an audit of all of its IT systems and classify them according to their potential for adaptation and their likely life-span. The audit should pay particular attention to those systems that could provide the basis for a single customer record across HMRC.

XV What progress has HMRC made?

XV.1 I am pleased to say that all the recommendations in this report have been accepted by HMRC. Of the 45 recommendations listed, HMRC has made progress on 39, implementing 13 of them. This is in addition to the actions already undertaken independently by HMRC outlined in section VIII.

XV.2 The table below sets out each recommendation, its status and timescale for being actioned. The Department will report on progress of these recommendations through its Data Security Programme, with the expectation that all recommendations will have been successfully implemented within the planned 24-36 month duration of the Programme.

Recommendation	Accepted	implemented	Started
R1 The role of information security as a corporate objective should be acknowledged by HMRC and work should immediately begin to formalise this objective within its mission and strategy(s).	✓	✓	
R2 Line of Business objectives for information security should be set to support the overall achievement of information security corporate objectives.	✓		✓
R3 HMRC's Business and IT Strategy should be updated to make them consistent with the direction of travel set out in this report.	✓		✓
R4 HMRC should initiate a review of any policies or legislation that might need to be changed if it is to be able to specify the manner in which its customers should interact with it.	✓	✓	
R5 HMRC should initiate an exercise to formalise its information security strategy, making sure it supports its updated Business and IT Strategy.	✓	✓	
R6 HMRC should identify 'quick wins' to set it off on the right direction of travel.	✓	✓	
R7 HMRC should identify and investigate initiatives which will take it further along the new direction of travel in the medium term.	✓		✓
R8 HMRC should seek to achieve a better balance between strategic and tactical investment.	✓		✓
R9 The HMRC Data Security Programme should start to coordinate and manage current security activities and initiatives as a coordinated, integrated body of work.	✓	✓	
R10 The Data Security Programme Board should be sponsored by an ExCom member and have members who are senior enough to ensure effective coordination and implementation.	✓	✓	
R11 HMRC should appoint a Chief Risk Officer.	✓	✓	

Recommendation	Accepted	implemented	Started
R12 HMRC should appoint a CISO at a senior level, reporting to the CRO.	✓		✓
R13 HMRC should establish a professional risk management function, whose roles should include supporting the Lines of Business in managing their risks through a common, Department-wide process, and supporting the CRO, the CFO and other ExCom members in the identification and assessment of strategic risks.	✓		✓
R14 The Chairman, Chief Executive, Chief Operating Officer and CFO and their senior advisers should use periodic meetings with the Directors-General of Lines of Business and their senior management teams as a forum to support and challenge the Lines of Business on information security.	✓		✓
R15 HMRC should engage its staff by communicating the direction of travel detailed in this report. This communication needs to recognise how far removed from today's reality this will seem and be alive to staff perception that HMRC's priorities constantly change and that this may therefore be initially viewed with a degree of scepticism.	✓		
R16 HMRC should commence the alignment of HR, Communications, Learning and change activities to ensure that information security policies and processes are embedded into day-to-day working life and behaviours.	✓	✓	
R17 HMRC should ensure that staff, at all levels, understand their responsibilities and accountabilities for information security and apply information security policies and principles in their day-to-day roles.	✓		✓
R18 Information security messages and controls should be incorporated into all employee life-cycle processes, from attraction and recruitment through to exit.	✓	✓	
R19 HMRC should develop and implement a information security awareness programme that includes regular refresher training to remind and update staff of the risks and of their responsibilities.	✓	✓	
R20 HMRC should build appropriate levels of capability in the management of information security across the Department.	✓		✓
R21 HMRC should consider using Pacesetter as the means of driving changes in behaviour around information security	✓		✓
R22 Information security guidance should be simplified, shortened and made more accessible	✓		✓
R23 Central guidance on information security policy and standards from S&BC should be translated by all Business Units into locally applicable procedures and the accountabilities between S&BC and the Lines of Business made clear.	✓		✓
R24 HMRC should enhance its S&BC capabilities to take a more proactive stance on incident management.	✓		✓

Recommendation	Accepted	implemented	Started
R25 HMRC should adopt a structured approach to assuring and auditing performance in relation to information security, based on the unambiguous accountability of Business Directors for information security within their areas of management control; assurance and audit activity carried out on behalf of Line of Business Directors-General; and corporate assurance and audit activity undertaken by the CISO and the CISO's staff.	✓		✓
R26 Each Line of Business should identify an information security sponsor on its Management Board and should appoint an information security professional to provide leadership for information security across the Line of Business.	✓		
R27 Each Line of Business should identify an appropriate risk management sponsor on its Management Board and should appoint a risk management professional to provide leadership for risk management.	✓		
R28 HMRC should ensure that the mechanisms that it provides for managing key linkages between interdependent functions, for example those between the Business Units and shared resources such as Customer Contact, Debt Management, IMS and ESS, are effective.	✓		✓
R29 The Data Guardian, and any professional information security role at the Line of Business level, should include explicit responsibility for the people-related aspects of information security.	✓		✓
R30 Each Line of Business should in the short term have a clear point of accountability for the security of mail handling, including the handling of mail by post-rooms owned by both ESS and itself.	✓		✓
R31 HMRC should make its access control consistent across all of its systems and estate.	✓		✓
R32 Each Business Unit should conduct a capacity review for paper storage to determine its future requirements so that it can be compliant with the clear desk policy.	✓		✓
R33 HMRC should map its end to end data flows at the right level of detail to enable effective information security risk identification and management.	✓		✓
R34 Service level agreements should be agreed to ensure that the service meets the operational needs of the business.	✓		✓
R35 HMRC should initiate a programme of Third Party Assurance in respect of information security requirements.	✓	✓	
R36 IMS should enhance the current approach to project approval for new IT systems (RMADS) to ensure that business owners understand the risks they are being asked to accept.	✓		✓
R37 IMS should initiate a review of the ASPIRE contract to determine whether it reflects adequate information security.	✓	✓	
R38 HMRC should urgently draw up its strategy for the replacement of Child Benefit systems and the transfer of the contract for Child Benefit IT Provision across from DWP.	✓		✓

Recommendation	Accepted	implemented	Started
R39 HMRC should move to an IT investment model that includes more of an emphasis on risk quantification.	✓		✓
R40 HMRC should strengthen business requirement specification, particularly around non-functional requirements.	✓		✓
R41 HMRC should enhance its business continuity management.	✓		✓
R42 HMRC should continue to move the emphasis from Business Unit commissioning of IT projects to corporate prioritisation of IT projects.	✓	✓	
R43 Build the business case for the new direction of travel outlined in this report, including determining the route map to get there, the timescales, and the level of investment required.	✓		
R44 HMRC should engage professional help to flesh out the new direction of travel, the business case behind it and the route map to get to it.	✓		
R45 HMRC should enhance the capabilities of IMS so that it is able to drive ASPIRE to deliver the enabling IT that underpins the direction of travel.	✓		

Appendices

A Poynter Review terms of reference

The terms of reference for this Review were published by HM Treasury on 23 November 2007. They are as follows:

"To establish the circumstances that led to the significant loss of confidential personal data on Child Benefit recipients and other recent losses of confidential data and the lessons to be learnt, and in the light of those circumstances to examine:

- *HMRC practices and procedures in the handling and transfer of confidential data on taxpayers and benefit/credit recipients;*
- *the processes for ensuring that these procedures are communicated to staff and the safeguards in place to ensure they are adhered to;*
- *the reasons why these failed to prevent the loss of confidential data;*
- *whether these procedures and processes are sufficient to ensure the confidentiality of personal data.*

The review will report initially by 14 December on the exact circumstances and events that led to the loss of the Child Benefit data, taking account of the ongoing investigation by the Metropolitan Police. It will make interim recommendations on any further, urgent measures that HMRC should put in place to guarantee the confidentiality of personal data.

The review will also consider wider implications, reporting in the Spring and, in consultation with the Independent Police Complaints Commission (IPCC) and Information Commissioner, make recommendations on:

- *how internal processes and culture can be strengthened to achieve appropriate data security in the future;*
- *whether HMRC's wider procedures for the handling of confidential data and liaison with other organisations should be changed to reduce the risks and how this might be done".*

Based on these Terms of Reference, I have agreed with HMRC and HMT that my review is focused on data loss and therefore excludes misuse of data – including any misuse of data held by HMRC by its staff.

I was appointed by the Chancellor to conduct this review and have provided my services free of charge. My team from PwC was procured by HMT though the Office of Government Commerce's Catalist Multi-Disciplinary Consultancy Framework Contract, which includes PwC's discounted rates for public sector work.

The review has delivered to the timescales and the budget pre-agreed with HMT. The forensic analysis involved in *The Investigation* has cost £0.6m and the *The Wider Review* has cost £3m. The latter has been a broad-ranging and detailed review and is summarised in this report. More detailed recommendations have been left and agreed with all fifteen Business Units visited. Further information on the work performed during *The Wider Review* can be found on page 53.

B Glossary of key terms and abbreviations

Term	Definition
ASPIRE	Acquiring Strategic Partners for Inland Revenue – the name given to HMRC's contract for IT services primed by Cap Gemini.
B&C	Benefits and Credits Department (HMRC department)
BRATS	Business Risk Analysis Tool for Security
CBCS	Child Benefit Computer System
CBO	Child Benefit Office (HMRC department)
CC	Claimant Compliance (HMRC department)
CFO	Chief Finance Officer
CISO	Chief Information Security Officer
CRB	Criminal Record Bureau
CRCA	Commissioners for Revenue and Customs Act 2005
CRO	Chief Risk Officer
CSSD	Corporate Shared Services Directorate (HMRC department)
Directorate	Business unit within HMRC
DSO	Departmental Strategic Objective
DSSM	Departmental Security Standards Manual
DTP	Departmental Transformation Programme
DWP	Department for Work and Pensions
EDS	Electronic Data Systems Limited, a third party IT services supplier
ESS	Estates and Support Services (HMRC department)
ExCom	Executive Committee, HMRC's Board
FSA	Financial Services Authority
HMCE	Her Majesty's Customs and Excise (joined with IR to form HMRC in 2005)
HMRC	Her Majesty's Revenue and Customs
HMT	Her Majesty's Treasury
I/We	During this review, Kieran Poynter has been assisted by a team from PwC. This is the team to which 'we' refers.
IDEA	Computer Software used for sampling and indexing
ICM	Integrated Customer Management (HMRC) programme
ICO	Information Commissioner's Office
IDG	Information Disclosure Guidance

Term	Definition
IMS	Information Management Solutions (HMRC department)
IPCC	Independent Police Complaints Commission
IR	Inland Revenue (joined with HMCE to form HMRC in 2005).
ISA	International Standard on Auditing
ISO/IEC 27001 and 27002	British Standards Institute's standards on information security
KAI	Knowledge and Intelligence (HMRC department)
L&G	Legal and Governance (HMRC department)
LMS	Learning Management System
MPPC3	Modernising PAYE Processes for Customers
NAO	National Audit Office
NICO	National Insurance Contributions Office
NIRS2	National Insurance Recording System 2
Pacesetter	HMRC change programme
PDE	Performance Development Evaluation
PwC	PricewaterhouseCoopers LLP
RMADS	Risk Management Accreditation Document Set
SA	Self Assessment
S&BC	Security & Business Continuity
SFIA	Skills for the Information Age
SIRO	Senior Information Risk Officer
STA	Service Transformation Agreement
SMS	Security Management Systems
SPOC	Single Point of Contact
Tax Post	Internal post system at HMRC operated by TNT
TCO	Tax Credit Office (HMRC department)
TNT	3rd party logistics company operating the HMRC internal post
URAC	User Requirement and Acceptance Criteria (data request form in use at HMRC)
WinZip®	Computer software used for file compression
WVP	Waterview Park, HMRC office in Washington, Tyne and Wear

C *The Investigation* approach

The *Investigation* phase of the Review has adopted the following approach in order to establish the circumstances and events leading to the loss of the CBCS discs containing the child benefit data:

(a) Identified nineteen relevant personnel at the offices of HMRC in Washington Tyne and Wear, London and Preston to be interviewed as witnesses based on its analysis of electronic and hard copy documentary evidence obtained;

(b) Conducted interviews with relevant personnel at the offices of HMRC in Washington Tyne and Wear, London and Preston in order to obtain an understanding of the events that took place and the roles played by those individuals. In most cases these interviews were conducted jointly with the IPCC;

(c) Held meetings with senior representatives of the NAO and conducted two interviews, in conjunction with the IPCC, with NAO staff involved in the audit of the CBO;

(d) Obtained the full current and backup email files of the witnesses and undertaken electronic analysis of these files using a defined list of search terms;

(e) Obtained and analysed the images of the hard drives of the two computers central to the circumstances leading to the data loss, and some additional discs contained within the secure locked room at HMRC premises in Washington Tyne and Wear; and

(f) Retrieved and reviewed a large amount of relevant hard copy documentation from HMRC, the IPCC, and the NAO, including the files provided by HMRC to the Metropolitan Police.

DOCUMENTATION

In the course of its work my team has compiled a selection of key original documents which are referenced throughout this report. These documents include copies of relevant emails, interview notes, policies and other such information identified during this investigation.

In the course of its investigations, my team has also compiled a number of working papers to assist and inform its work, some of which have been shared with representatives of the IPCC and HMRC. These working papers are not included as attachments to this report, though the key findings have been extracted and summarised herein.

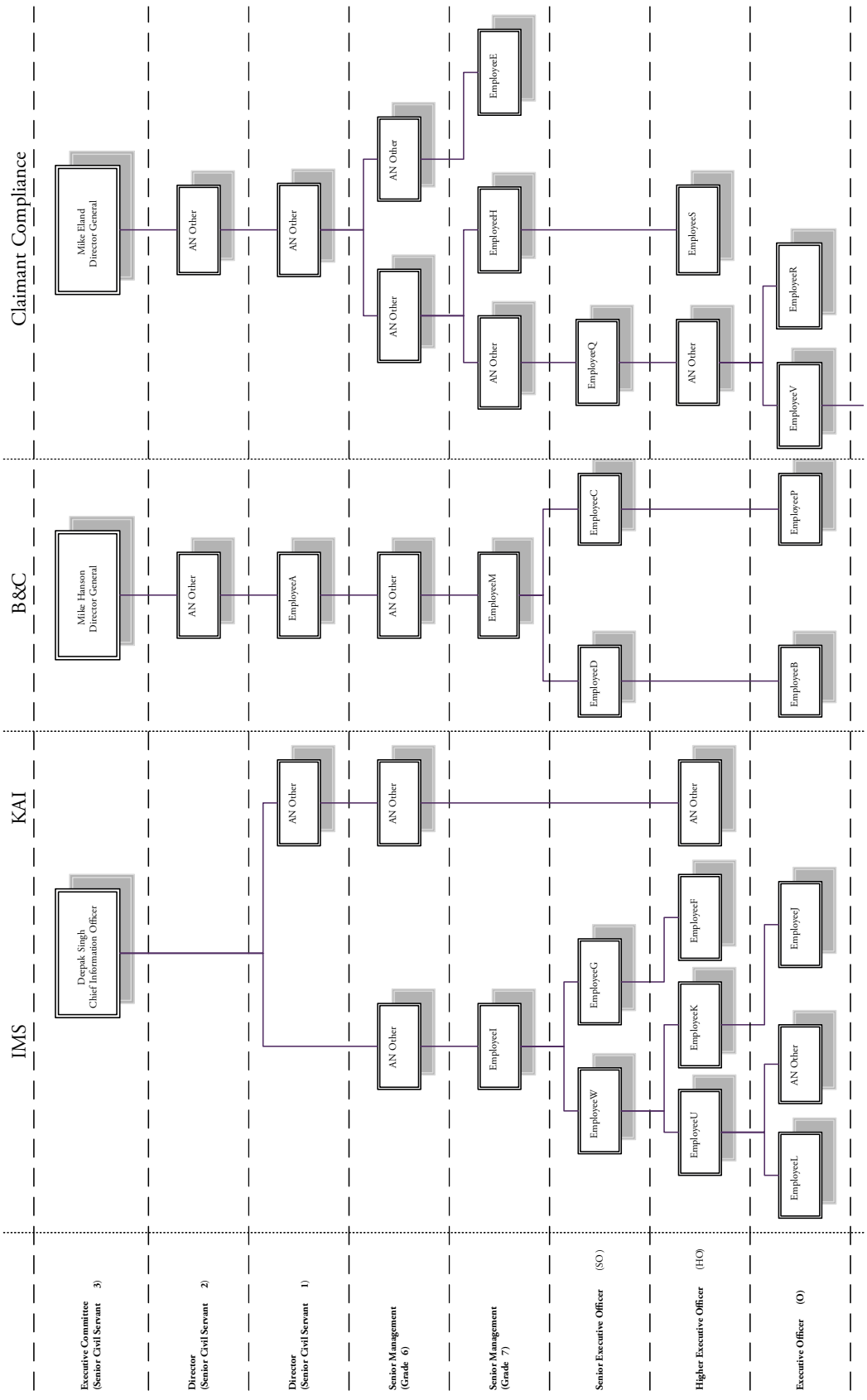
INTERVIEWS

My team has largely conducted its interviews with witnesses in conjunction with the IPCC. All interviewees were offered the choice of having the interviews recorded, but all but one interviewee declined this option, preferring to have notes transposed by hand. The interviewees have since been provided with copies of the transposed notes for authentication and approval.

COMPUTER FORENSIC ANALYSIS

We obtained and reviewed the contents of the e-mail files for relevant HMRC personnel. However, due to entirely unavoidable circumstances, my team was not able to conduct a full forensic analysis of the email files of two of the witnesses to the events leading to the loss of the CBCS data. The backup data of these two mail files had become corrupted, as often occurs in similar organisations with significant IT infrastructure, rendering the data inaccessible despite my team's best efforts to retrieve it. In addition, certain older email files from other witnesses were not retrieved from electronic archives stored elsewhere within HMRC's IT infrastructure. Taking account of the entirety of the evidence gathered and made available to my team, I do not believe that these minor limitations are likely to have had a material effect on the overall findings.

D Organogram of relevant individuals in HMRC



E Diagram of key events leading to the loss