Audit Committee 9 December 2009

Response to the Poynter Review and Cross Government Actions: Mandatory Minimum Measures

Executive summary and recommendations

Introduction

Since the major information loss at HMRC in November 2007 HPC have evaluated current security arrangements, and reported on the current state of play in December 2007, and subsequently at Audit Committee in March 2008.

In June 2008 the governments' response, "The Poynter Review" was published, following the in depth examination around the business processes, understanding of Risk, and Information Security at HMRC; and the issues surrounding the data loss.

At the same time numerous other incidents in the public and private sector in the UK, US and elsewhere, have continued to keep information security in the public view. The UK's Information Commissioner has now been given the power to fine organisations, and "audit public sector bodies without prior notice".

As a responsible regulator, HPC has evaluated the 'Poynter Review', "Cross Government Actions: Mandatory Minimum Measures", Sir Gus O'Donnell, June 2008 and other guidance, and have taken appropriate measures as outlined in the presentation attached, and detailed in the document Response to the Poynter Review and Cross Government Actions: Mandatory Minimum Actions.

Decision

Audit Committee is asked to discuss the attached presentation and report and Approve HPC's recommendations

Background information

Presentation - The Poynter Review. Implications for Information & Data security at HPC (Roy Dunn & Greg Ross-Sampson) 9th December 2009

Review of information security at HM Revenue and Customs. Final report. Kieran Poynter (Poynter Review) June 2008

Resource implications
Some small scale reassignment of duties around information security within departments may be required. There is no growth in head count predicted around this part of the project. See Response to the Poynter Review and Cross Government Actions: Mandatory Minimum Measures (20091109iQUARPTInformation Security Recommendations – Master copy) which is attached.

Financial implications
Preparation of ISO27001 Information Security Standard and BS25999 Business Continuity standard, will cost approximately £15,000 plus VAT for contractors assistance and is in the 2010-11 work plan and proposed for budgetary approval.

Training requirements for internal auditors and lead audit functions are being determined, but would be spread across two financial years.

The BSI assessment and initial certification costs, predicted for the year following implementation of the Information Security and Business Continuity Management systems (2011-12) will cost approximately £10,000 plus VAT and will be included in the 2011-12 workplan.

Appendices
Response to the Poynter Review and Cross Government Actions: Mandatory Minimum Actions (20091109iQUARPTInformation Security Recommendations – Master copy) Roy Dunn & Greg Ross-Sampson

Date of paper
12th November 2009.

Response to the Poynter Review and Cross Government Actions: Mandatory Minimum Measures

Introduction

Following an initial report on the Poynter Review delivered 10th November 2008, EMT have requested that The Poynter Review is responded to in the same manner as the CHRE report on the NMC from last summer. Namely every action or review point R 1 – 45 is addressed even if it is not directly relevant to HPC.

The Poynter Review also prescribes four roles to manage information risk and governance. Models of how similar roles could be established without employing more headcount have been devised.

Analysis of physical security of buildings and the paper archive are also underway, and are included toward the end of this report.

The "Cross Government Actions: Mandatory Minimum Measures" documents the central governments approach to information security following the review by Sir Gus O'Donnell June 2008.

A further report "Protecting Government Information. Independent Review of Government Information Assurance "The Coleman Report" Commissioned by the Cabinet Office was also published in June 2008. This report looks at key principles of accountability and Risk. This is not included, but can be supplied if you wish.

Additional items are included in this report.

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.

Suggested HPC response

HPC Executive considers information security to be a high priority for the council. This is illustrated by HPC's actions following the initial publicity around the HRMC data loss in 2007 and subsequently in 2008.

HPC's work plans will now include specific items concerning information security for each department.

A new role of "Chief Information Security Officer" is being created and will be responsible for ensuring that an information security objective is effectively propagated through HPC

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.

Suggested HPC response:

HPC's work plans will now include specific items concerning information security for each department, that reflect the achievement of the overall Corporate objective.

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.

Suggested HPC response

HPC's IT strategy already encompasses data security in a core objective :

"Information Technology Objective 3:

To protect the data and services of HPC from malicious damage and unexpected events.

This addresses the following strategic issues:

- The need for the organisation to quickly become operational following a major disaster to the premises or services;
- To protect the information services from malicious damage; and
- To secure the data collected and created by HPC from loss or theft. This risk is highlighted following the loss of personal data by the United Kingdom government in 2007."

The concepts of data security will be added at department level to strategies and workplans with the aid of Business Process Improvement

All future IT based projects will incorporate a specific information security risk analysis, and sign off of the implied risks around implementation of that particular project.

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.

Suggested HPC response

HPC may wish to proactively encourage registrants and applicants to use online systems for secure communication as these core functionalities become available.
Excluding the use of paper based mechanisms, may not be possible in the short to medium term, without legislative change.

The current online renewals, and future online applications projects, along with the existing online contact management system all move HPC toward improved security of registrant and applicant information.

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 an 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.

Suggested HPC response

An Information Security Strategy will be created by the new Chief Information Security Officer. It will bring together the aims and goals of HPC as a whole and address the specific points raised above.

The HMRC model will be evaluated and a matrix management approach developed to support information security across the organisation.

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 R33. 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.

Suggested HPC response

The mapping of basic data flows has already been completed for operational departments. These flows are included in the appendices section

The banning of unencrypted media removal from the HPC offices (with the exception of back up tapes) is being evaluated. The needs of personal or confidential information security are different from those of public information available for publication. Encryption is a potential dis-benefit where presentations are to be given off site.

- The HPC understanding is that the core physical forms for Registration and Renewals forms a contract with the HPC upon which an individuals registration is based. We therefore retain the original signed forms for legal admission whilst scanned versions of the forms are used for operational processes
- The HPC will instigate a tactical manual encryption process for transferring any data on removable media (except backups). The HPC already encrypts all Laptop computers
- The HPC are developing internet based services to allow Registrants to renew electronically rather than by using paper forms. Currently Registrants are able to make address changes electronically.

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.

Suggested HPC response

The push toward electronic communications as opposed to paper based channels is already being pursued (online renewals and online applications ultimately). Online address changes are already possible for all registrants.

Paper forms for Renewal and Registration are currently scanned on receipt and the paper copy stored using a specialist archival company to support the legal requirements of the business process.

Following the deployment of the Online Renewal service we predict that there will be an increase in the communication exacted electronically via email. The HPC will analyse the use of this new service after several professions have completed their renewal cycles to inform future developments to capitalise on this communication channel.

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.

Suggested HPC response:

The HPC has a history of investing for the longer term as evidenced by the projects to develop the core registration application NetRegulate and now the Online Renewals application. The HPC five year plan also indicates when significant investment into the organisation is planned to support the continued development of the HPC.

The HPC does not have the same issues with islands of information as the HMRC. It appears that the HMRC runs several related and similar processes independently in business silos resulting in discrete islands of information. The HPC has a single regulatory objective separated into discrete functions i.e. Registration, Approvals, Fitness to Practice each has clearly separate business processes with only a small subset of common data. There already exist basic mechanisms to control the propagation of data between systems for example the FTP system ‘pulls’ address information from the NetRegulate ‘master’ record.

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.

Suggested HPC response:

The HPC executive is evaluating options for progressing information security management throughout the organisation. The above references will be used as a baseline for HPC's requirements. A list of requirements to support the information security function at HPC will be developed.
Awareness programmes, training and testing are being designed to support the goal of improved information security.

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").

Suggested HPC response :

This structure reflects the complexity of HRMC as an organisation. The functions of the roles highlighted, Senior Information Risk Officer (SIRO), Chief Risk Officer (CRO) Chief Information Security Officer (CISO), Data Guardian (DG) have been evaluated and used to build roles for HPC's use. HPC is a flatter structure organisation, where line management feeds directly into EMT.

The role of Senior Information Risk Officer (SIRO) will not be filled.
The Director of Operations will take on the responsibilities of Chief Risk Officer (CRO).
The Head of Business Process Improvement will take on the responsibilities of Chief Information Security Officer (CISO).

A full mapping of HMRC's Information and Risk management, and HPC's version is provided at the end of this document at Appendix 4

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.

Suggested HPC response

At HPC the Director of Operations will fulfil the function of Risk Officer from May 2009 onwards

Typically the responsibilities of a CRO are as follows (from Wikipedia 2009**)**;

The **Chief Risk Officer** is the organizational "risk champion" accountable to the CER for ensuring that the risk management strategy has been effectively embedded into the organisation. As the sponsor for all risk management activities, the CRO is responsible for ensuring that risk management and performance management have been integrated by all levels of HPC and all key risks are being escalated up the chain of command accordingly.

The **Chief Risk Officer** will be accountable to the CER. He/she will ensure that the HPC Governance Processes are fit for purpose, operating and effective and ensure that current and emerging risk is identified, managed, monitored, reviewed and documented

This role will advise EMT and the Council on risk strategy and policy, oversee the implementation of a consistent, integrated risk management framework throughout the organization, Central oversight of the organization's risk assessment and risk appetite.

The Director of Operations reports to the Chief Executive and Registrar.
HPC is a medium sized organisation and cannot justify a FTE just to be responsible for Risk. The Head of Business Process Improvement currently reports risk to the HPC Audit Committee on a day to day basis.

(Risk has previously resided with the Director of Finance and most recently the Secretary to Council.)

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.

Suggested HPC response

Establishing a single person to be responsible for all security is not costly or complex. However they will need to have a broad knowledge of Data, Information use and law, Information Technology use, business processes, and buildings security.
HPC's Head of Business Process Improvement will take on the responsibilities of CISO. The Head of Business Process Improvement already reports to the Director of Operations who holds the Risk portfolio at HPC. This emulates the reporting structure at HMRC
HPC is a medium sized organisation and cannot justify a FTE just to be responsible for Information Security. This will therefore be a significant but not isolated part of the role of Head of Business Process Improvement.

No Job or role description is currently available from HMRC, however the current incumbent, (a former Information Security consultant at PWC) has provided the following information. (PriceWaters Coopers (PWC) authored the Poynter report.) The JD is reproduced in full at the end of this document at Appendix 2.

> "The CISO advises and assists the governing bodies and Business Units in the fulfilment of their responsibilities, including action in relation to chain of trust agreements, business continuity and disaster recovery plans, and audit and governmental compliance practices.
>
> The CISO responsibilities encompass all aspects of information security, including action to establish the infrastructure and organisational culture that is needed to meet the information security objectives."

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.

Suggested HPC response:

HPC is a medium sized organisation and cannot justify a FTE just to be responsible for Risk. The Director of Operations will fulfil the function of Risk Officer from May 2009 onwards? The Head of Business Process Improvement will manage the day to day function of Risk Reporting.

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.

Suggested HPC response

All business function heads report to the Chief Executive or his direct reports. Information security can be addressed on an ongoing basis over the course of a working year via EMT and CDT meetings, plus 1 to 1's.

Any significant new risks around information security will be escalated to the Chief Executive immediately upon discovery and a response planned. Serious information security risks may have to be addressed and other projects may need to be postponed or cancelled should urgent remediation be required.

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.

Suggested HPC response:

An across HPC education plan will be developed, and will be delivered by a combination of All Staff meeting presentations, online (HPC Network based) training resources and team meeting discussions. Employee information security will be used to illustrate how information loss could impact applicants and registrants. This programme will require long term support by all business areas.

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.

Suggested HPC response:

Information security is discussed in several settings during the new starter induction process which aims to embed the principles of information security early on in the working relationship. During the Human Resources induction employees are asked to read the IT Policy and sign to say they accept and understand the terms of use of IT systems and security and to read and sign a data protection statement. They also have an induction with their manager which includes the following topics as part of the minimum checklist: use of Information Technology, computer networks and email system; procedures for HPC document control; use of IT equipment; and security arrangements. Subsequently they are also required to have inductions with each department at the HPC which allows for a more detailed and focussed briefing from the IT department and Operations Directorate. These structured approaches ensure consistency of communication across all employees. As IT is an ever-innovating and changing environment there may be occasions when all-employee presentations or communications are necessary to update on the latest best practice or security measures.

R17 HMRC should ensure that staff, at al 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.

Suggested HPC response:

HPC approach: Ensure HPC's Information security policy is easy to understand, and of a length that does not make it too much to understand and absorb.
Assign / appoint an experienced employee within each department to be the local lead on information security. This person will work with the head of department to evaluate existing security arrangements and access requirements for ongoing operations.
See R16.

R18 Information security messages and controls should be incorporated into al 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.

Suggested HPC response:

The HPC undertakes the following pre-employment checks in respect of all contract and permanent roles: references, qualifications, third party obligations, right to work in the UK and CRB disclosure for Fitness to Practise Department employees. The offer of employment letter and contractual documentation refer to information security, intellectual property rights, data protection and confidentiality requirements which they must agree to in accepting employment with the HPC. [See R16 in terms of induction of new employees]. On leaving the HPC there is an exit process which sets out in writing the employee's responsibilities in respect of return of documents and equipment which is overseen by the employee's manager on their last day.

For recruitment of temporary workers employed by agencies, the right to work in the UK is checked and a data protection form is provided on their first day of work for them to read and return signed.

R19 HMRC should develop and implement an 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.

Suggested HPC response:

There is not currently a refresher programme for employees on information security but this could be incorporated into all-employee meetings 1 – 2 times per year to enable employees to be reminded, or updated, on policies and processes and to keep the issue in the forefront of employees' minds.

Network based training mechanisms are currently being tested / about to be tested in the Registration department. If successful, these mechanisms will be extended to support ongoing information security training. Training resources are being developed for use with this channel of training.

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.

Suggested HPC response:

This structure reflects the complexity of HRMC as an organisation and its ability to absorb new roles as required. HPC is a flatter structure organisation, where line management feeds directly into EMT. Where recruitment of information security based roles is not feasible, best practice training will be provided to support development of the roles indicated.

The Director of Operations will take on the responsibilities of Chief Risk Officer.

The Head of business Process Improvement will take on the responsibilities of Chief Information Security Officer.

All of the key information security roles will be supported by specific best practice training within two years, namely; ISEB Certificate in Information Security Management Principles; ISEB Information Risk Management / OGC Management of Risk training.

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.

Suggested HPC response:

I think we would need to see if/what behaviours need changing before we can say if Pacesetter would be an appropriate response for the HPC.
* Workplace process for clear desk and disposal of confidential waste will be developed where appropriate; a version of this is currently in place.
•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) will be highlighted via ISO audit procedures;
* Written procedures for data transfers will be enhanced;
* Data Guardian's will take part in the review of work procedures;
* Adding information security as a standing agenda item at weekly performance meetings; and
* Information security will be automatically included in all project planning as a checkpoint prior to acceptance of any Functional Specification.

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.

Suggested HPC response:

The Information Security policy is part of the IT policy and the Confidentiality policy with a total length of 8 pages and are written as a set of principles rather than a list of rules. The policies are available through the Intranet and the HRInfo system; all employees are required to sign the IT policy prior to be given access to information systems.

Guidance with regard to the secure disposal of electronic records will be added to the policy.

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 DSSM1 1235 and DSSM1 1240. 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.

Suggested HPC response:

HPC will broadly follow the principles of ISO27001 Information Security Standard and BCS Information Security Management Principles, and may implement certification against this standard for some areas of the business in the future.

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).

Suggested HPC response:

All information security incidents will be recorded to a central location, investigated, root cause analysis carried out, and ongoing risks of repeat occurrence assessed, and mitigated against where possible. A Risk free environment is not possible with mobile workers, off site hearings, and online systems.

Information security forums and conferences will be monitored for perceived threats and vulnerabilities; however this does tend to raise the number of potential incidents considered,

This may appear to involve a loss of time to attending vendor hosted meetings where the deliverable content is unpredictable.

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.

Suggested HPC response: HPC will adopt ISO27001 information security standard as an example of best practice that can be tailored to our requirements. Whilst HPC may not attempt to gain certification against this standard until at least 2010-11, specific certified information security training will be arranged for those involved in the programme. Whilst the standard is being adopted, this will provide a set of auditable guidelines against which we can measure ourselves.

EMT members will have oversight of information security within their line of business, whilst the Business Process Improvement function will provide guidance, best practice advice and reporting of information security effectiveness. Information Security will be reported to the audit Committee on an ongoing basis.

Information Security Qualifications will be obtained in appropriate areas, for instance Certificate in Information Security Management Principles, (British Computer Society & Information Systems Examination Board)

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.

Suggested HPC response: Each member of EMT will take responsibility for information security for their line of business. They will be assisted by Business Process Improvement to assess information risks and evaluate potential changes to existing processes to mitigate these risks where appropriate.

Day to day advice to employees within the business will best be provided by an experienced business user of the data within the department. The experienced user will know the use to which the data can legitimately be used, the threats posed by loss of that data, and the other parts of the organisation which may have access to that data. This role is that of the Data Guardian.

Data Guardian is a specific role from the Poynter Review.

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.

Suggested HPC response

HPC is a medium sized organisation and appointment of a Risk professional would be overly expensive and disproportionate. Risk will be established as part of the Director of Operations role/ Head of Business Process Improvement role. This will include advising on Risk matters with the executive, and reporting to the Audit committee
A description of the Risk role will be produced based on the output from the Poynter Review. HMRC Corporate Governance have supplied the requirements for these roles, which have been tailored to our size of organisation, and our remit.

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.

Suggested HPC response:

The approach indicated by HMRC is known broadly as either Single customer Record or Customer Relationship Management within the IT industry. HPC Business Process Improvement will evaluate the potential benefits and disbenefits of taking a CRM approach to data handling. This will be in the form of a report on CRM principles and a Single Customer Record within HPC.

The output of this report will be a description of current existing data flows, an evaluation of future data flows, estimates of record numbers, and potential methods for decreasing re-keying or transferring data manually around the organisation. HPC currently does not have the additional vulnerability of disparate offices, or regular transfers of bulk personal data to other organisations.

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.

Suggested HPC response

The appointment of an information security professional or data guardian to each department or line of business would be disproportionate to the size of HPC and the current level of risk it faces.

However EMT members will be responsible for overall lines of business, with an experienced line manager or team leader with knowledge of local business practices acting part time as Data Guardian.

A generic role description will be produced relating to Line of Business Data Guardian. This can be appended to appropriate job descriptions. Some specific training may be required for all those acting as Data Guardians. This will be obtained or developed by the CISO role.

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.

Suggested HPC response:

HPC, as a medium sized organisation keen to control growth of costs, must balanced against security requirements against levels of risk.
A single post room is in place with highly experienced employees in place. The major departments expecting mail provide additional assistance when in peak periods. Individual post rooms are not a practical solution for HPC. However, additional security within the post room will be provided. A lockable post box for potentially sensitive mail to be stored overnight will be provided in the next 12 months. HPC wide building security is being enhanced with secured office areas, requiring security pass controlled access and tracking.
Hard copy mail will always be vulnerable to loss or tampering as it passes through systems external to HPC.

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.

Suggested HPC response

The HPC operates a multi-tier authentication and authorisation mechanism by requiring all IT users to first logon to the Network and then to logon to a specialised application e.g. NetRegulate, Mail service etc where further authorisation determines what parts of the application and data are accessible to each individual.
IT is notified of leavers and transfers via the HR new starters and leavers form at which point accounts are closed, archived or allowed access by specific authorised individuals.

Reporting against an individuals access rights can be achieved although it is not a trivial exercise and should be considered by the Information Security Officer role.

Access rights to buildings are controlled by a combination of personalised photo-id card provided to all full time employees. Temporary employees will also require photo-id cards in future as access through out the building will be further controlled by swipe card terminals on all non public areas. See section "Supplementary items to be included in this review" concerning physical security.

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.

Suggested HPC response:

The move away from the use of paper has commenced with online renewals and application developments. Where possible communication is carried out by electronic means. Hard copy documents are scanned, linked and destroyed where possible.
Hard copy confidential or personal details are always stored in locked cabinets overnight or when not in use.
However some processes are still entirely paper based, and where these contain no personal or confidential information, desk storage will be allowed due to the limited amount of lockable storage we wish to have on the premises.
It is envisaged that over the medium term paper usage will fall, and even applications and renewals will be simply scanned and linked, with paper being securely destroyed as opposed to stored.

The Fitness to Practice department is likely to continue to use paper documents in the short to medium term, and adequate lockable storage is currently provided. Growth in throughput of cases will require additional storage, and this will be provided. Temporary lockable storage can be provided by the use of Transit cases.

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.

Suggested HPC response:

HPC has already mapped the key flows of data around the organisation, and to offsite service providers, printers, solicitors and parliamentary agents.

These flows, together with the Quality processes using these data will be used to locate potential security shortfalls, and these will be addressed as they are discovered.
A mechanism will be established within the Project Management function to ensure changes to IT applications or data structures are verified against information security requirements.
Changes to industry best practice may influence the information security of individual types of data. For instance the PCI DSS standard for credit and debit card information has caused a move from "retain data to prove that we were authorised to charge the card account" to "retain minimal data and harden the security around those data that are stored,"

Such sea changes in perceived best practice will require financial and human resources to implement within appropriate time scales.

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.

Suggested HPC response:

The HPC IT department is planning to review the Service Levels it publishes in the 2009/10 year. This will be done taking into account known information security requirements.

The HPC will formalise the policies regarding information exchange between external organisations and the HPC.

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.

Suggested HPC response

HPC will use its existing ISO9001:2000 processes to audit all external suppliers handling sensitive information, other than where those suppliers have achieved ISO9001:2000 or ISO 27001 certification in their own right.
HPC has already undergone an evaluation of many of its suppliers (January 2008). The existing archive provider has been unable to accommodate our enhanced security requirements and will therefore be replaced following intensive contract negotiation with potential replacement suppliers.
Whilst some cost savings will be achieved long term the main criteria for supplier selection has been enhanced intrinsic security.
It will be necessary for the user departments to assist in any external service provider audit. The audit of major data handlers will be addressed first.

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.

Suggested HPC response

Risk within each project or enhancement to an IT system or paper based system will be evaluated and recorded at the commencement of the project, and confirmed at the end of the sign off of the functional specification. As a general principle IT developments should enhance overall information security and decrease levels of information security risk.
Project sponsors will actively accept any additional risks associated with the proposed project and subsequent activity required to run the new processes or applications resulting from those new activities..
Risks will be monitored throughout the project lifecycle, and any additional level of risk be escalated (by the Project Management function) to the Project Lead for consideration.

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.

Suggested HPC response

The ASPIRE contract relates specifically to an outsourcing contract for “Inland Revenue” IT services. This has since been increased to incorporate a wider remit with HRMC.
HPC do not currently operate outsourcing contracts of a similar nature, although some systems are externally developed and maintained.
Data transfer is not required for development and support activity by external suppliers.
User Acceptance Testing (UAT) of new registration system functions occurs on servers in house, without any public access.

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.

Suggested HPC response

HPC does not use a Child Benefit system and does not need to interoperate with external systems, operated by other organisations.

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.

Suggested HPC response:

HPC does not operate in an environment where estimation of financial impacts of risks would be helpful. One of the greatest threats is reputation risk associated with significant information loss.

Our legal advisors, Bircham, Dyson Bell have suggested insuring against cost of £50,000 would mitigate against any additional High Court costs that we may incur due to a data loss issue.

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.

Suggested HPC response:

A set of default non-functional requirements addressing information security will be developed with the Project Management and IT functions. These will form a default set of non-functional requirements for all future IT base projects.

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 25AW4 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.

Suggested HPC response:

HPC's business continuity provision is flexible and aims to provide our basic services to protect the public within a realistic time frame and Information assets are protected via two channels. Data is replicated to our existing ISP, and backed up to data tapes, which are stored in a fire proof safe.

There is a small risk that changes to IT architecture result in some data not being backed up. However planning for changes in infrastructure around project work incorporates evaluation of DR/Business Continuity requirements. The IT department operates a "Change Management" process based on the industry standard ITIL (Information Technology Infrastructure Library). Accidental damage to HPC's business Continuity provision is therefore unlikely.

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 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.

Suggested HPC response:

The HPC executive reviews all Major and Small project developments as part of the annual financial cycle and so has an holistic view of the impact across business areas from system developments and is able to prioritise accordingly.

HPC's project prioritisation process highest ranking criterion is around information security. This ranking has been in place since 2006.

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.

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).

Suggested HPC response:

A direction of travel for HPC can broadly be considered as follows;

- Secured online access for registrants, applicants and stakeholders to improve security and legitimate accessibility.
- Multiple communication channels, with the preferred channels being highlighted and made most attractive to use.
- Enforced rules for data integrity and security, based on industry best practice.
- Single customer view or Customer Relationship Management or at least shared data via selective development of application interfaces and reporting.

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 re-deploy 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.

Suggested HPC response:

HPC have published an IT Strategy since 2004, taking a medium term (5 year) view. This is updated every year. This strategy looks at the short to medium term requirements to support and develop the business functions of HPC and accommodate changes to legislation and the scope of regulation.

Scalability, reliability and security are the other key factors featuring in the ongoing strategy. Online, non paper based processes are being developed as the preferred methods of contact with applicants and registrants.

Any major IT development has been assessed by NCC, our current Penetration testing contractor, to determine the appropriate levels of security required. This is now built into the design of the system from the functional specification onwards.

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.

Suggested HPC response:

This is a specific action point for the HMRC driven by the loss of data that reflects specific remedial actions; there is no perception that the HPC has a similar Risk.

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.

Suggested HPC response

The ASPIRE contract relates specifically to an outsourcing contract for "Inland Revenue" IT services. This has since been increased to incorporate a wider remit with HRMC.

HPC do not currently operate outsourcing contracts of a similar nature, although some systems are externally developed and maintained.

Supplementary items to be included in this review.

Person, building, and archive security are not specifically included in the Poynter review. However it is prudent to determine our direction on these issues also.

Physical Security

Person Security

Essentially we need to determine if a person needs access to the building fabric as a contractor, access as a visitor to the public areas of the building for meetings, or requires access to the office areas of the building, and access to the information within.

All persons requiring or having access to information within HPC should have references checked, by the HR department, and have a name, job title and photograph published on the intranet before they commence employment. This will assist in determining if new faces within the building are visitors, employees or others.

The name and published photograph of the person using the security pass should be flashed up to the Reception desk as confirmation that the pass is being used by the correct person. Access via the rear door should theoretically be possible via a similar system, displayed to the Reception Desk area monitors.

It is unrealistic to expect employees to challenge all unknown faces around the building if there is a high likelihood that they could simply be visitors, new employees or contractors.

This will be partially mitigated when all employees and short to medium term contractors are required to wear their security pass at all times. (See building security below).

Building Security

HPC is a “public” organisation that aims to be open and transparent where ever possible. We are required to invite members of the public, contractors, registrants, partners and other stakeholders into our premises as part of our function.

However, we should be able to prevent non employees being able to wander freely around the premises to any area. Non employees should be restricted to those areas they have a legitimate business reason for access. Similarly, employees can tailgate others entering the building and their passage is not recorded, whilst exit from the building is not recorded at all. We cannot be considered secure if we do not know who is in the building.

HPC must ensure that anyone with access to any of the building is authorised to be on the premises, and their access is recorded and time stamped. Medium to long term, security barriers such as those used in the Underground and other secure buildings may be required.

At present there is no way of forcing visitors to scan their visitor badges on the way out of the building if they are retaining them for the following day. (Should they retain them themselves, or should the badge be stored in reception at HPC?) If the visitor looses the badge whilst outside the building, an intruder could possibly gain entry to the building fraudulently.)

The impact of such access is that an unauthorised person could attend a private meeting or access confidential data, steal from employees or visitors, or attack employees or visitors.

One possible mechanism to force visitors and employees to “sign in and out” would be to use a gate system such as that used in large commercial buildings and the Rail and Tube networks. There are space constraints, and the reception area would need to be moved or

redesigned. The image attached here indicates a standard set of barriers. Such items are used at the GMC's shared office space in Euston.

This may well be going too far for HPC but is the only way of ensuring compliance with the requirement to log ones self in and out of the building, person by person. A simpler way would be to have swipe devices to open the doors to leave the premises in the same way as we currently have them to enter. These could also be in place in the proposed restricted areas.

Subdivision of the HPC Campus

As a regulator we are required to hold large amounts of information on individuals registered with HPC, and also hold the usual range of HR, Finance information on employees and contractors.

Much of this information is confidential or private.

To protect this information it is suggested that two levels of building security are created.

Public area security – includes all those areas where meetings, hearings and public events take place. This will include the reception area, all meeting rooms, corridors and toilet areas, and the kitchen in Park House.

CCTV monitoring will be available if required for Hearing areas, no confidential documents or information will be stored in these locations, and will only be used when the business owner of that information is present.

Transit cases may be used on a temporary basis should overnight storage of Hearings materials be required. However the Transit cases will be stored in the FTP area which will have Confidential area security.

Confidential area security – includes all those areas where data and information is stored or processed. This is essentially all "office space", Park House floors 1,2,3; covering Fitness to Practice, Education, Policy departments; Basement, covering Finance, and Post Room; Ground floor covering Information Technology and Human Resources; Stannary Street, Registrations, Communications and Secretariat and Mezzanine floor, HR Partners, Operations (including Business Process Improvement and Projects).

Human Resources, Information Technology and Finance departments will have access restricted to department members outside normal business hours. (8am-6pm).

These areas will have locking doors, and electronic security passes will be required to gain entry to these areas outside business hours. Only Finance, HR, IT department members have access to their office areas outside normal business hours. (8am-6pm)

A map of the probable access control units is provided at the end of this section of the document. Some areas such as lifts and staircases will be very difficult to secure, and where this proves impossible, other solutions must be found.

These areas will operate a clear desk policy as far as personal information is concerned. Adequate amounts of secure (lockable) storage must be provided to accommodate all paperwork

Key management for lockable storage must be implemented to allow access to keys during occasions of holiday and unexpected sickness. This could be based around a lockable post box for keys near the exits to the building.

Keys would be retrieved first thing on the next business day by the Facilities department, and be released to those having business reasons for access.

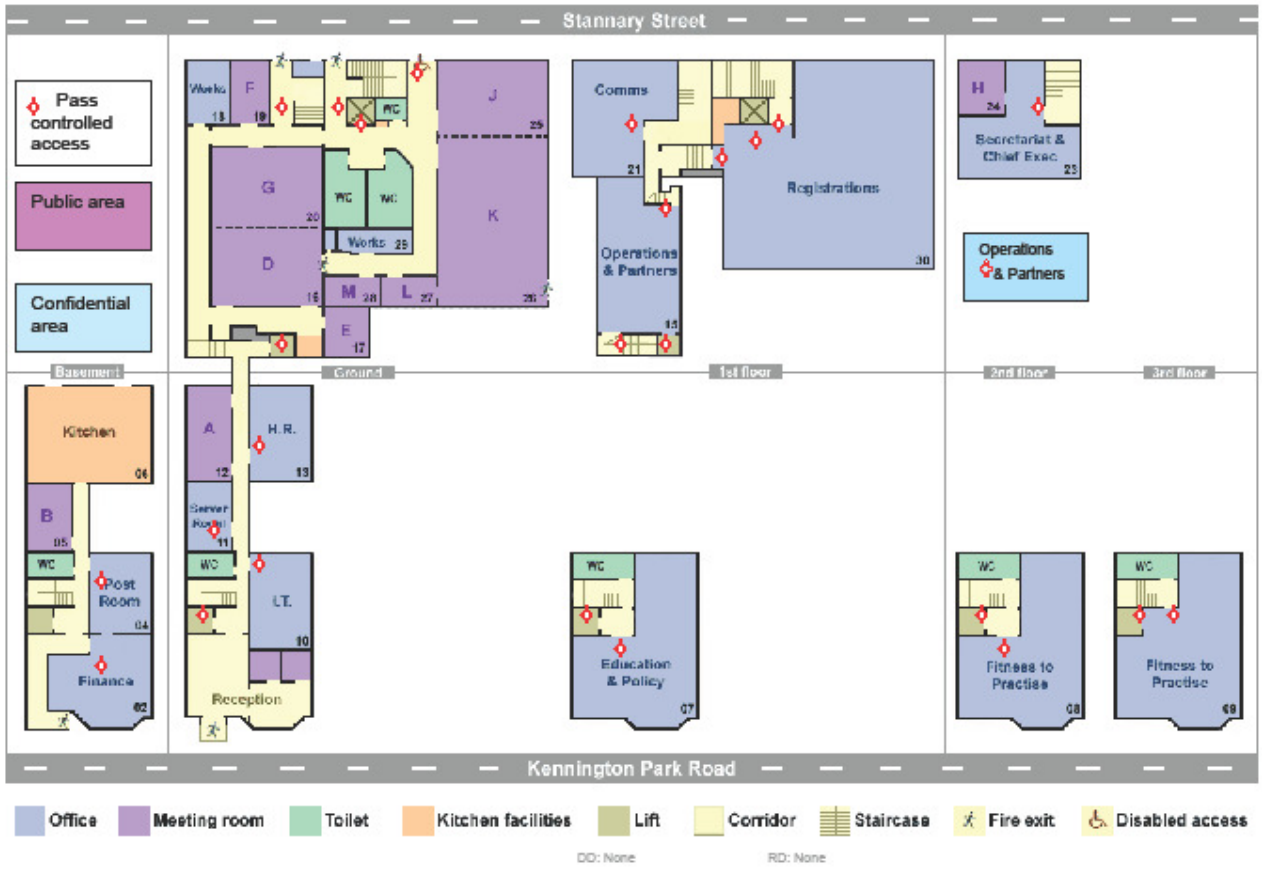
Some areas cannot be secured due to the construction of the building. For instance the Mezzanine area is currently impossible to secure, without investment of approximately £100 k. This area may be converted to meeting room space when the Phase two building works are completed on 22-24 Stannary Street.

The Park House lift currently opens directly onto the third floor Fitness to Practice area. This area contains highly confidential data, and is one of the least secure parts of the HPC campus.

If the Park House lift cannot be hardened to allow secure access only, the most appropriate mitigation will be to swap the Education and Policy departments currently residing on the first floor, with the FTP third floor occupants.

This will place (Education & Policy) information requiring less secure storage, in the area of lower physical security, and FTP data requiring the greatest levels of physical security in a more secure area.

In the mean time adequate levels of secure, lockable storage must be provided to allow the clear desk policy to be implemented.


Stannary Street
Pass controlled access
Public area
Confidential area
Basement
Ground
1st floor
2nd floor
3rd floor
Kitchen
Post Room
Finance
Reception
H.R.
Server Room
LT.
Education & Policy
Comms
Registrations
Operations & Partners
Secretariat & Chief Exec
Fitness to Practise
Kennington Park Road
Office
Meeting room
Toilet
Kitchen facilities
Lift
Corridor
Staircase
Fire exit
Disabled access
DD: None
RD: None

Impact of increased security on non employees at HPC

HPC periodically engages temporary workers on contract via an employment agency. Up to the end of March 2009, those temporary workers expected to be on site for less than 6 weeks were not issued their own security pass.

With the implementation of the two levels of building security indicated above, all temporary workers will require individual passes as soon as their contract with HPC commences.

Contractors will also either need temporary security cards to pass through the secured doors, or have an employee with them at all times.

Further tightening of security could be achieved by restricting access to different work areas to those working in the departments located on those floors. For instance only Registrations advisors have access to the Registrations department. However this may be too restrictive at this stage.

Contractors

Royal Mail postal workers collect and deliver direct to the post room after passing through the reception area. They do not sign in. They are recorded on the reception area CCTV. The Post Room/Facilities office when secured will either need to be occupied to allow the Royal Mail operative access, or have Reception release the door remotely for the post person.

We also need to determine what to do about contractors working outside normal business hours.

Our cleaning contractors work from approximately 7pm to 10 pm and are not supervised at all by HPC employees. They have access to anything left on desks, and could easily remove equipment or paperwork if it is not secured.

Our window cleaners usually work only in daylight hours and are on site from 07.30 hrs onwards when most of the office is empty. If the clear desk policy is not implemented, there is a significant risk of information loss.

Our confidential shredding contractor has access to much information already via the material they are required to collect on our behalf. However again we are trusting external contractors to go around our office space unsupervised. Is this a reasonable thing to do? A decision is required, and mitigation put in place if we allow continued unsupervised access.

Security of the HPC paper Archive

HPC stores approximately 3000 cartons of applications for registration, completed renewal notices, Fitness to Practice case information, HR records and Finance records with a commercial archiving contractor.

Whilst the archiving industry views security as an important issue, some archive locations are intrinsically more secure than others.

Many archiving companies use anonymous warehouses to store material. Such warehouses can be the subject of speculative robbery attempts, and in the last two years two supposedly secure archive sites have been burned to the ground. Although complex fire detection systems are in place, the local fire brigade will not attempt to extinguish the fire unless persons are believed to be in danger. Thus, sophisticated fire detection systems are not necessarily an indicator of satisfactory reaction to a fire.

However HPC's primary requirement is around information security rather than preservation.

Much material is now created and stored electronically, negating the requirement for a hard copy original, other than for theoretical legal reasons.

HPC's preferred archiving provider uses a salt mine in Cheshire as its primary site. This site in inherently safer than the usual warehouse type building. Mine access controls are in place, and transit down the mineshaft is required via lift to access the storage area. The main security risk with any archive provider is around the transport of the items from HPC to the warehouse location.

Anonymous trucks and vans are preferable to branded vehicles, discouraging data theft. Insurance against loss of archive material in transit can also be obtained, although financial recompense is no mitigation against reputation damage.

Transport of Confidential material between HPC and our scanning service

In 2008 Business Process Improvement implemented increased security of confidential material in transit between HPC and our current scanning supplier Service Point.

Archive cartons of information to be scanned is locked in custom made transit cases. These cases are used to transport the items to be scanned (box, within a box, within a box principle) and have been used successfully by Registrations, Communications and Secretariat departments.

The Fitness to Practice department will commence electronic delivery of files for printing to a service deemed to be sufficiently secure for HPC's use in the short term, and the Business Process Improvement function will audit the service when it is up and running.

Poynter's Ten Principles of Information Security

Poynter proposes 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 rationalized 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.

Cross Government Actions: Mandatory Minimum Measures

Government has put in place a core set of mandatory minimum measures to protect information, to apply across central Government. They are minimum measures in that they oblige individual Departments and agencies to assess their own risk, and those organisations will often put in place a higher level of protection. They will be updated in the future to accommodate lessons and new developments.

1.
Information is a key asset, and its proper use is fundamental to the delivery of public services. The public are entitled to expect that Government will protect their privacy and use and handle information professionally. Departments are best placed to understand their information and to protect it, but need to do so within a context of clear minimum standards ensuring protection of personal information.

2.
This document sets out in Section I mandatory process measures to ensure that Departments identify and manage their information risks. In Section II it sets out mandatory specific minimum measures for protection of personal information. It does not cover physical and personnel security or business continuity, which are addressed in the Manual of Protective Security, which is under review. Departments must also comply with other obligations, such as those under contracts, codes of connection, and the law. The material in this document reflects good practice as set out in the ISO/IEC 27000 (Information Security Management System) series.

Section I: Process measures to manage information risk
General
3.
Departments are responsible for managing their own information risks and ensuring proper management of information risks in their delivery chains, subject to meeting the mandatory rules set out in this document and its replacements. The Accounting Officer has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. They sign the annual Statement of Internal Control. From 08/09 onwards, this must explicitly cover information risk.

4.
All Departments must:

4.1
have an information risk policy setting out how they implement the measures in this document in their own activity and that of their delivery partners, and monitor compliance with the policy and its effectiveness;

4.2
assess risks to the confidentiality, integrity and availability of information in their delivery chain at least quarterly, taking account of extant Government-wide guidance, and plan and implement proportionate responses, which must at least include implementation of the measures in Section II. At least once a year, the risk assessment must examine forthcoming potential changes in services, technology and threats;

4.3

accredit ICT systems handling protectively marked information to the Government standard, and to reaccredit when systems undergo significant change, or at least every five years;

4.4
conduct Privacy Impact Assessments so that they can be considered as part of the information risk aspects of Gateway Reviews, or while going through accreditation if no Gateway has been conducted for a particular system;

4.5
use the security clauses from the Office of Government Commerce's model ICT contract for services, with any changes relevant to information risk being approved by the SIRO (defined below);

4.6
consider whether each Section I measure needs to be applied to any organisation handling information on its behalf (whether public sector or private sector) to ensure appropriate information handling across the delivery chain, and apply those where there is a need to do so;

4.7
apply all Section II measures by organisations handling information on their behalf when they deal with Government data, and monitor the application of those measures. When seeking to apply Section I or Section II measures, Departments must insist on action where they can, and seek to influence others where necessary.

Roles

5.
All Departments must:

5.1
name a board member as “Senior Information Risk Owner” (SIRO). The SIRO is an executive who is familiar with information risks and the organisation’s response. The SIRO may also be the Chief Information Officer (CIO) if the latter is on the board. They own the information risk policy and risk assessment, act as an advocate for information risk on the board and in internal discussions, and provide written advice to the accounting officer on the content of their Statement of Internal Control relating to information risk; [R10 in Poynter]

5.2
identify their information assets, and name for each an “information asset owner”. Asset owners must be senior individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process; and [part of R33 in Poynter]

5.3
identify and keep a record of those members of staff and contractors with access to or involved in handling individual records containing protected personal data (see attachment A), referred to below as “users”. For simplicity, some Departments may wish to assume that all staff are users, or to conduct the exercise for their organisation piece by piece. [Not currently included as an action for IT, although user access is specifically controlled via]

Maximising public benefit from information

6.
Addressing information risk involves ensuring that information is used, as well as protecting it when it is used. Information Asset Owners must consider on an annual basis how better use could be made of their information assets within the law. Where they consider that public protection or public services could be enhanced through greater access to information held by others, they should submit a request to the relevant Information Asset Owner. Requests received must be logged and considered.
Where it is decided that public access to information is in the public interest, Information Asset Owners should reflect this in their Departmental Freedom of Information Publication Scheme.

Audit

7.

All Departments must:
7.1
share and discuss the information risk assessment (see 4.2) with their audit committee and main board;

7.2
conduct at least an annual review of information risk for the SIRO to support their written advice to the Accounting Officer. That review must cover the effectiveness of the overarching policy. It must be informed by the written judgement of the Information Asset Owners, and chair of the audit committee; and

7.3
once the Statement on Internal Control has been completed, share the relevant material and the supporting annual assessment with Cabinet Office.

Culture

8.

All Departments must:
8.1
have and execute plans to lead and foster a culture that values, protects and uses information for the public good, and monitor progress at least though standardised civil-service wide questions when conducting a people survey or equivalent;

8.2
reflect performance in managing information risk into HR processes, in particular making clear that failure to apply Departmental procedure is a serious matter, and in some situations amount to gross misconduct; and

8.3
maintain mechanisms that command the confidence of individuals through which they may bring concerns about information risk to the attention of senior management or the audit committee, anonymously if necessary, and record concerns expressed and action taken in response.

Incident management

9.
All Departments must:
9.1
have a policy for reporting, managing and recovering from information risk incidents, including losses of protected personal data and ICT security incidents, defining responsibilities, and make staff aware of the policy; and

9.2
report security incidents to HMG's incident management schemes (GovCERTUK for network security incidents and CINRAS for incidents involving cryptographic items). Significant actual or potential losses of personal data should be shared with the Information Commissioner and the Cabinet Office.

Transparency

10.
All Departments must:
10.1
publish an information charter setting out how they handle information and how members of the public can address any concerns that they have;

10.2
set out in the Departmental annual report summary material on information risk, covering the overall judgement in the Statement on Internal Control, numbers of information risk incidents sufficiently significant for the Information Commissioner to be informed, the numbers of people potentially affected, and actions taken to contain the breach and prevent recurrence.

Section II: Specific minimum measures to protect personal information
11.

Government must be particularly careful to protect personal data whose release or loss could cause harm or distress to individuals. All Departments must:

11.1
determine what information they or their delivery partners hold that falls into this category. This must include at least the information outlined at A; and

11.2
handle all such information as if it were at least “PROTECT – PERSONAL DATA” while it is processed or stored within Government or its delivery partners, applying the measures in this document. Information should continue to be marked to a higher level where that is already done or where justified for example as a result of aggregation of data.

Preventing unauthorised access to protectively marked information

12.
When PROTECT level information is held on paper, it must be locked away when not in use or the premises on which it is held secured. When information is held and accessed on ICT systems on secure premises, all Departments must apply the minimum protections for information set out in the matrix in the Annex, or equivalent measures, as well as any additional protections as needed as a result of their risk assessment. Where equivalent measures are adopted, or, in exceptional circumstances in which such measures cannot be applied, the SIRO must agree this action with the Accounting Officer and notify Cabinet Office.

13.
Wherever possible, protected personal data should be held and accessed on paper or ICT systems on secure premises (see other documents within the MPS), protected as above. This means Departments should avoid use of removable media (including laptops, removable discs, CDs, USB memory sticks, PDAs and media card formats) for storage or access to such data where possible. Where this is not possible, all Departments should work to the following hierarchy, recording the reasons why a particular approach has been adopted in a particular case or a particular business area:

13.1
the best option is to hold and access data on ICT systems on secure premises;

13.2
second best is secure remote access, so that data can be viewed or amended without being permanently stored on the remote computer. This is possible at PROTECT level over the internet using products meeting the FIPS 140-2 standard or equivalent, or using a smaller set of products at RESTRICTED level. The National Technical Authority for Information Assurance, CESG, provides advice on suitable products and how to use them;

13.3
third best is secured transfer of information to a remote computer on a secure site on which it will be permanently stored. Both the data at rest and the link should be protected at least to the FIPS 140-2 standard or equivalent, using approved products as above. Protectively marked information must not be stored on privately owned computers unless they are protected in this way;

13.4
in all cases, the remote computer should be password protected, configured so that its functionality is minimised to its intended business use only, and have up to date software patches and anti-virus software.

14.
Where it is not possible to avoid the use of removable media, all Departments should apply all of the following conditions:

14.1
the information transferred to the removable media should be the minimum necessary to achieve the business purpose, both in terms of the numbers of people covered by the information and the scope of information held. Where possible, only anonymised information should be held;

14.2
the removable media should be encrypted to a standard of at least FIPS 140-2 or equivalent in addition to being protected by a authentication mechanism, such as a password;

14.3
user rights to transfer data to removable media should be carefully considered and strictly limited to ensure that this is only provided where absolutely necessary for business purposes and subject to monitoring by managers and the Information Asset Owner; and

14.4
the individual responsible for the removable media should handle it – themselves or if they entrust it to others – as if it were the equivalent of a large amount of their own cash.

15.
There are some exceptional situations in which the second condition of encryption cannot be applied consistent with business continuity and disaster recovery. For example, full system back-up tapes must contain all the relevant data and Departments may judge that encrypted data cannot be recovered with sufficient speed or certainty in the event of a disaster. Such unprotected data include some of the most valuable assets owned by a Department, and should be treated accordingly, being recorded, moved, stored and monitored with strong controls– equivalent to handling arrangements for very large amounts of public money in cash. There are also specific situations in which Departments hold removable media that they cannot encrypt for legal reasons, such as when such material is collected in evidence for a legal proceeding. In those situations, the legal obligation prevails.

16.
All material that has been used for protected data should be subject to controlled disposal. All Departments must:

16.1
destroy paper records containing protected personal data by incineration, pulping or shredding so that reconstruction is unlikely; and

16.2
dispose of electronic media that have been used for protected personal data through secure destruction, overwriting, erasure or degaussing for re-use.

17.
Decisions on handling on the issues in paragraphs 13 – 16 should be approved in writing by the relevant Information Asset Owner. In preparing for the annual assessment of information risk, all Departments must:

17.1
review compliance with the matrix in the Annex or equivalent measures and any SIRO decision to take other action agreed with the Accounting Officer;

17.2
review and test documentation relating to decisions made relating to paragraphs 13 – 16;

17.3
inspect a sample of the activities of those individuals with rights to transfer protected personal data to removable media, to ensure that there is still a business case for them to have those rights;

17.4
inspect a sample of those individuals who have left roles with access to protected personal data, to ensure that access rights have been removed;

17.5
inspect a sample of removable media to ensure that required safeguards are in place;

17.6
inspect unencrypted back-ups (see paragraph 15) and reconcile them with material that has been recorded;

17.7
monitor disposal channels for paper records containing protected personal data to ensure this has been properly handled; and

17.8
ask for sample electronic media to be processed as in 16.2 and testing to attempt data recovery.

18.
All Departments whose delivery chain involves the handling of information relating to 100,000 or more identifiable individuals must engage independent experts to carry out penetration testing of their ICT systems and to make recommendations.

Minimising risk from authorised access to protectively marked information

19.
All Departments must ensure that all data users must successfully undergo information risk awareness training on appointment and at least annually. In addition, all Information Asset Owners must pass information management training on appointment and at least annually, and accounting officers, SIROs, and members of the audit committee must pass strategic information risk management training at least annually.

20.
All Departments must plan their business taking into account the information risks involved in different business models as well as their benefits. Once a business model is adopted, Departments must explicitly define and document the access rights granted to protected personal data that users enjoy, and minimise access rights within the adopted model. The Information Asset Owner must agree in writing that access rights permit the business to be transacted with an acceptable level of risk, and if not, an alternative must be identified. Access rights should be minimised in respect of each of the following:

20.1
pool of records accessible. The default should be that any member of staff has no access to protected personal information. If access is necessary, it should be to the smallest possible sub-set of records;

20.2
numbers of records viewed. The hierarchy should be no access / ability to view only aggregated data / ability to view only anonymous records / ability to view material from single identifiable records / ability to view material from many identifiable records simultaneously;

20.3
nature of information available. The hierarchy should be responses to defined queries (e.g. does X claim free school meals) without seeing the record / view of parts of the record itself / view of the whole record; and

20.4
functionality, including searching, alteration, deletion, printing, downloading or transferring information.

21.
All Departments must:

20.5
put in place arrangements to log activity of data users in respect of electronically held protected personal information, and for managers to check it is being properly conducted, with a particular focus on those working remotely and those with higher levels of functionality. Summary records of managers' activity must be shared with the relevant Information Asset Owner and be available for inspection by the Information Commissioner's Office on request; and

20.6

have a forensic readiness policy to maximise their ability to preserve, analyse and use evidence from an ICT system, should it be required.

Citizen-facing work
22.
Departments and agencies need to ensure that citizen facing services are secure, while being easy for people or their representatives to use. Where possible, the same protective measures should be taken in transacting business with individuals as when information is stored or used within Government, but Departments should set their own proportionate standards in this area so long as those standards (and possible alternatives service routes) are clearly explained.

Minimum scope of protected personal data

Departments must identify data they or their delivery partners hold whose release or loss could cause harm or distress to individuals. This must include as a minimum all data falling into one or both categories below.

A. Any information that links one or more identifiable living person with information about them whose release would put them at significant risk of harm or distress.

1. one or more of the pieces of information which can be used along with public domain information to identify an individual	**combined with**	**2. information about that individual whose release is likely to cause harm or distress**
Name / addresses (home or business or both) / postcode / email / telephone numbers / driving licence number / date of birth [Note that driving licence number is included in this list because it directly yields date of birth and first part of surname]		Sensitive personal data as defined by s2 of the Data protection Act, including records relating to the criminal justice system, and group membership DNA or finger prints / bank, financial or credit card details / mother's maiden name / National Insurance number / Tax, benefit or pension records / health records / employment record / school attendance or records / material relating to social services including child protection and housing
Core applicants and registrants identity and contact details,	HPC data	FTP data, data provided for initial proof of identity when applying for registration, employee and some contractor details, partner and council member details

These are not exhaustive lists. Departments should determine whether other information they hold should be included in either category.

B. Any source of information about 1000 or more identifiable individuals, other than information sourced from the public domain.

This could be a database with 1000 or more entries containing facts mentioned in box 1, or an electronic folder or drive containing 1000 or more records about individuals. Again, this is a minimum standard. Information on smaller numbers of individuals may warrant protection because of the nature of the individuals, nature or source of the information, or extent of information.

Suggested HPC response: All information within HPC and its business partners will be classified into the two categories above.

APPENDIX 1 Accountabilities & Responsibilities mapped to HPC

The various accountabilities and responsibilities indicated by Poynter are listed. The proposed HPC equivalent is indicated in the [square brackets] highlighted in yellow.

1. In her capacity as **Principal Accounting Officer**, the CEO has formal responsibility (evidenced in the annual Statement of Internal Control) for maintaining a sound system of internal control which manages the key risks to the achievement of the Department's policies, aims and objectives.

[HPC mapped equivalent - Chief Executive and Registrar (CER)]

- As head of the Department, the CEO has a key role to play in promoting and supporting the risk management strategy.
- To provide the lead to enable HMRC to meet its stated aim of becoming the best risk management organisation in the public sector, comparable with the best in the private sector.
- To review the risk management strategy and give final approval by signing off the document.
- To undertake *Government Accounting* responsibilities for ensuring effective governance and risk management systems are maintained to support the achievement of the organisation's business objectives.
- To sign the *Statement on Internal Control*, which reflects the outcomes of the Department's strategic approach to risk management

2. The **Board (Executive & Advisors Committee)** is responsible:

[HPC mapped equivalent – Council & EMT]

- To set, communicate and review the Department's strategic direction.
- To approve the risk management strategy and subsequent revisions
- To set and communicate the Department's priorities and values, including the commitment to governance and embedded risk management.
- To consider risk management issues and reports from the Board's sub-committees, deciding on all unresolved issues.

3. The **Executive Committee** role is to ensure:

[HPC mapped equivalent – EMT]

- Ensure that there is a robust framework in place to identify, monitor and manage HMRC's strategic risks and opportunities

- Responsible for the management and quarterly review of the Departmental Risk Register following the QSR
- Receive regular reporting on key Departmental risks and identify necessary actions
- Determine HMRC's risk appetite level for each of its high risks
- Promote and oversee the implementation of the Risk Management strategy
- Identification and management of key Departmental risks
- Allocate resources to the Departmental Risk Register action plan

4. The **Chief Finance Officer (CFO)** is the Departmental "risk champion" accountable to the CEO for ensuring that the risk management strategy has been effectively embedded into the Department. As the sponsor for all risk management activities, the CFO is responsible for ensuring that risk management and performance management have been integrated by all levels of HMRC and all key risks are being escalated up the chain of command accordingly.

[HPC mapped equivalent – Director of Operations with responsibilities of the CRO. Responsibility for Finance remains with Director of Finance at HPC]

5. **Directors General (DG)** are accountable to the CEO.

[HPC mapped equivalent – EMT, owners of lines of business]

They are responsible for:

- Ensuring that risks to the achievement of their objectives are identified, assessed and managed effectively.
- To incorporate the management of the key risks into delivery of the DG/Chief level *Business Plan* objectives.
- To ensure appropriate *Directorate-* and *Programme-level risk registers* are established and necessarily maintained.
- To obtain appropriate assurances that effective risk management and internal control processes are in place to support delivery of their DG objectives
- They are accountable for risks delegated downwards from Departmental level
- They are responsible for ensuring that a robust risk management framework has been implemented and operating effectively within their line of business.
- The DGs are responsible for setting the acceptable levels of risk tolerance for risks managed at portfolio level.
- They are responsible for escalating risks beyond their DG control to ExCom level when required.
- Supported by their respective Business Risk Partners, they must ensure that any cross cutting risks are being jointly managed appropriately.
- They must appoint a lead "risk champion" to facilitate the embedding of the risk management framework throughout their line of business. The "risk champion" must be a SCS level either a Finance Director or a Director.

- To encourage risk management as a key competency for senior-level staff.

6. In turn, **Directors** are accountable to their DGs for risk management within their Directorates.

[HPC mapped equivalent – EMT, owners of lines of business]

They are responsible for:

- Ensuring that an effective framework is in place to manage risks faced by the directorate.
- Identify and agree new risks and opportunities and identify owner/ manager.
- Identify and analyse risks for impact and likelihood and introduce risk control measures.
- Ensure directorate risk register is accurate and up to date.
- Monitor progress of planned actions on a quarterly basis to ensure aims are achieved.
- Report quarterly to the respective Business Risk Partner on progress of risk management action plans and any new risks identified.
- Report on the Directorate risk register via the Monthly Performance Pack and quarterly via the Quarterly Strategic Review.
- Communicate the risk process to all staff and ensure they are aware of their responsibilities.
- Identify initiatives that could reduce impact and/or likelihood of risk
- Escalating risks that fall outside the Directorate control or the appetite level up to DG level for consideration

On a monthly basis the top risks should be reviewed and actions updated by the Directorate management team and the respective risk owners. They are responsible for setting the risk appetite level for their area and therefore must evaluate the cost of mitigating the risk against the appetite level.

7. **Directors and assistant directors** have a key role in promoting the open and honest culture to underpin effective risk management, and need to ensure that the key risks are visible, owned and actively addressed by management. They are also required to provide assurance that key risks have been effectively managed.

[HPC mapped equivalent – EMT, owners of lines of business]

The Assistant/deputy directors are responsible for actively managing the operational risks, reviewing key risks on a regular basis and providing updates to the Directors.

8. The **Lead Risk Champion** is appointed by the DG to facilitate the roll out of the risk management framework within their respective line of business. They will be supported by the Business Risk Partners and have a direct reporting line either to the DG or a Director. The LRC will act as the conduit between the Corporate Risk Management Group and the business. They will review and challenge any escalated risks and provide monthly updates to the DG. The LRC will ensure that risk management is been consistently applied across the LoB through periodic risk based testing.

[HPC mapped equivalent – Director of Operations with ISO Audit function]

9. The **Risk Owner** is assigned to a risk that needs to be actively managed.

[HPC mapped equivalent – EMT & line of business owners, Heads of Departments]

They are responsible and accountable for:

- Owning the risk assessment and response to the risk;

- Management of risk, including implementation of action plans;
- If the risk is critical or it is on the Corporate Risk Register than an update on the actions must be provided either via the Monthly Performance Pack or the Quarterly Strategic Review;
- Report any deviation from profile of risk to the respective Business Risk Partner;
- Monitoring the risk where there is material change in its status;
- Provide regular reporting to the risk partners.

10. **Managers** are accountable for ensuring that all staffs play a key role in understanding the risks they face.

[HPC mapped equivalent – EMT, owners of lines of business, Heads of Department and Team Leaders]

- They are accountable to the Assistant Director to ensure that all key risks have been identified and there are appropriate controls in place to mitigate these risks.
- They are responsible for capturing any key risks, near misses or incidents occurring in their areas.
- They must ensure there is regular review of their key risks and that the controls are effective both in terms of operational and design.
- As and when a risk has been assessed as beyond their control, this risk must be escalated up Directorate when appropriate.

11. **The Corporate Risk Management Group** will have responsibility for taking an overview of risks facing HMRC and ensuring effective risk management.

[HPC mapped equivalent – EMT, ISO Audit function]

The group will:

- Challenge the effectiveness of risk management and risk mitigation in HMRC
- Support senior management in establishing the risk appetite
- Monitor compliance with HMRC's risk policy
- Periodically review the effectiveness and appropriateness of the risk management and reporting process
- Recommend future generic or specific measures to reduce risk
- Monitor and steer the management of existing risks
- Identify new risks and allocate ownership
- Escalate and report material risks issues to ExCom and the Board

The CRMG will meet on a monthly basis, to review all the key risks in the Departmental Risk Register (DRR). The Group will use information from individual Directors and DGs, as well as ExCom and the other sub-committees, to consider whether other emerging risks need to be formally tracked. In reviewing risks, the Corporate Risk Management Group assess the impact of individual risks in relation to achievement of DSOs and other business objectives.

Membership of the Corporate Risk Management Group will be attended by Lead Risk Champions, Business Risk Partners, Head of Corporate Risk Management and Director of Internal Audit. Chief Risk Officer will chair the committee and will provide a report to ExCom following every meeting with a view of significant current and emerging risks. If necessary, the Chair can alert ExCom to significant changes in risk exposure at any other time. ExCom may consider risks through specific slots on their agenda and may refer risks and handling strategies to the Board for assurance and advice.

The Corporate Risk Management Group will inform the Audit & Risk Committee of changes to the risk profile of the Department.

12. The **Quarterly Strategic Review Panel** will hold participants to account on whether their business will be delivered in line with HMRC's Ambition. The reviews will be strategic and forward looking. They will cover the latest outlook for the business and the key issues/risks that could prevent the achievement of key strategic targets/objectives.

[HPC mapped equivalent – EMT, owners of lines of business, ISO Audit function]

The Chief Executive Officer will chair the Reviews supported by the Chief Operating Officer, Chief People Officer, Chief Finance Officer and Director, FP&A. Participants, who

will be seen individually, are the Directors General, Chiefs, VOA Chief Executive and the Chief Executive Group

Meetings will be quarterly, typically in the last week of the month after the quarter end. The reviews will be informed by issues from the Performance Committee

Participants must provide members with a quarterly management information pack that covers the full scope of their business. The Chair will report back to the Executive Committee on the outcomes of the Review at the first meeting after the quarterly performance reviews have been conducted

13. The **Audit & Risk Committee is a sub-committee of the HMRC Board. It will meet bi-monthly.**

[HPC mapped equivalent – Audit Committee]

It is supported by Internal Audit and informed by the work of National Audit Office. It is responsible for:

- Providing assurance to the Board and the Principle Accounting Officer the efficacy of risk management and the strength and appropriateness of control processes across HMRC
- To advise the Board and POA on the strategic processes for risk and governance and the Statement on Internal Control;
- To review areas of risk escalated via the DRR;
- To review areas of risk referred by the Board or ExCom for in depth review, challenge and assurance;
- To review areas of risk regarded as high profile carrying significant reputational risk and external interest e.g. information security;

14. The **Internal Audit team** is responsible:

[HPC mapped equivalent – Business Process Improvement team including ISO9001 audit function]

- For providing an independent and objective opinion to the Chairman on risk management, control and governance, by measuring and evaluating their effectiveness in achieving HMRC 's agreed objectives;
- Supporting the identification of risk and improvements to the risk management process;
- To ensure compliance with established policies (including behavioural and ethical expectations), procedures, laws and regulations;
- Add value by providing best practice and engendering continuous improvement;

- The Director of Internal Audit provides the Chairman with an objective evaluation of, and opinions on, the effectiveness of HMRC's risk management, control and governance arrangements which informs the completion of the annual Statement of Internal Control

15. The **Chief Risk Officer** will be accountable to the CFO. He/she will ensure that the HMRC Governance Processes are fit for purpose, operating and effective and ensure that current and emerging risk is identified, managed, monitored, reviewed and documented

[HPC mapped equivalent – Director of Operations = CRO will be accountable to CER]

This role will advise ExCom and the Board on risk strategy and policy, oversee the implementation of a consistent, integrated risk management framework throughout the Department, Central oversight of the organization's risk assessment and risk appetite.

16. The **Corporate Risk Management team (CRMT**) will report to the Head of Corporate Risk Management. Their primary role will be to maintain both the HMRC Risk Management Framework and the Departmental Risk Register. Their responsibilities include:

[HPC mapped equivalent – Risk owners with input from Internal and External audit functions]

- Monitor and review the effectiveness of the risk management strategy;
- Develop and provide training to all involved in risk management activities;
- Develop strategies to measure and manage risks and opportunities;
- Develop risk management tools and processes;
- Communicating risk management information to all staff;
- Reporting to ExCom and the Performance Committee on all Departmental risks and key control issues;
- Responsible for ensuring that the Departmental Risk Register is kept up to date and all actions are monitored and reported to ExCom on a regular basis.
- All new emerging risks escalated up from the DG level will be reviewed and challenged by the CRMT before inclusion into the Corporate Risk Register;
- The team will inform the Performance Committee of any new entries in the HMRC risk register;
- Aggregate and analyse all risks considered to be HMRC wide;
- They will work closely with the Business Risk Partners in supporting the identification, analysis and appropriate management and mitigation of risks across the Department;

- The team will also act as a liaison point with internal and external stakeholders, and support the Business Risk Partners in putting the principles into practice;
- CRMT will maintain the risk management site on the Department's Intranet which acts as a focal point for written advice, guidance tools and good practice;

17. **Business Risk Partners** will

- Support the Directors and the DGs in embedding the risk management policy and procedures throughout their respective line of business;
- Build a risk aware culture including appropriate education and training;
- Assessing the risk management framework and process and disseminating lessons learnt
- They will work with the businesses to resolve control and audit issues;
- Building relationships with all key stakeholders including other risk partners in the Department;
- Maintain and review the DG and Directorate Risk Register;
- Coordinate the quarterly risk and control review;
- Developing appropriate risk responses;

They will be located at DG level reporting either to the Finance Director or an equivalent SCS level manager.

18. **Operational Risk Officers** will be located within the Business Units, supporting the line managers in embedding the risk management framework. They will be responsible for maintaining and reviewing the Business Unit Risk Register on a monthly basis, perform risk assessment and analysis, monitor control actions, escalate risks where appropriate and provide management with regular risk and control reports.

[HPC mapped equivalent – Team Leaders and Managers, or highly experienced team members within lines of business. Also act as Data Guardians]

19. While risk management requires central level coordination, the management of risk must be embedded at operational level which means **everyone in HMRC** must assume responsibility of identifying and escalating risks when appropriate.

- Staff are best placed to ensure that risks are considered at all time whenever normal duties are conducted.
- By identifying what could stop an individual from completing their task will allow line management to address any control issues and prioritise resource as appropriate.

- Within their given area of responsibility and work, have an understanding of risks and regard their management as part of their everyday activities, including identification and reporting of risks and opportunities which could affect HMRC
- Assist in or carry out risk assessments for their areas of work
- Maintain an awareness of risk and feed this into the formal management and reporting processes
- Support and participate in risk management activities where required.

Managers should encourage and support staff in the identification and discussion of risk in their day to day business, and pro-actively deal with issues that are brought to their attention, informing senior managers where appropriate

APPENDIX 2 Chief Information Security Officer Job Description based on PriceWaterhouse Coopers specification

Position Purpose

The security of information is critical to HPC and one of their primary corporate objectives. In the face of active threats, a changing risk picture, stronger control environment and more rigorous compliance, the role of Chief Information Security Officer (CISO) has become vital to the success of the organisation. Working under the authority of HPC with functional responsibility for information security, the CISO will develop the HPC information security strategies, policies, programmes and procedures, and provides leadership for their implementation and maintenance.

The CISO advises and assists the HPC governing bodies and Business Units in the fulfilment of their responsibilities, including action in relation to chain of trust agreements, business continuity and disaster recovery plans, and audit and governmental compliance practices.

The CISO responsibilities encompass all aspects of information security, including action to establish the infrastructure and organisational culture that is needed to meet the HPC information security objectives.

Key Responsibilities

- Provides strong professional leadership of the Information Security team, forward looking and focussed on good practice for information security.

- Develops and obtains agreement through HPC of the Information Security Strategy which ensures the HPC data is kept secure within an acceptable risk / cost model; addressing the integrity, confidentiality and availability of information assets.

- Responsibly for establishing the principles of the information risk appetite for HPC.

- Responsible for establishing processes for the assessment of information security, and ensuring HPC is aware of the risks inherent in acceptance of residual risk.

- With Heads of Business Units identifies the key issues to be addressed by each Business Unit in order to achieve HPC's corporate objectives for information security, and advises and assists Heads of Business Units in addressing those issues.

- Advises HPC on the governance and organisation of activities relating to information security, including advice on the information security implications of any major structural changes in the Department and on the roles and organisation of key information security positions such as that of Data Guardian.

- Directs staff in identifying, developing, and maintaining information security policies, processes, and practices throughout the organisation, and in providing functional leadership for their implementation, to reduce risks, respond to incidents, and limit exposure and liability in all areas of information risk.

- Specifies individual projects, and integrated Departmental programmes, to address information security issues, and leads or participates in the governance of those projects and programmes as required in order to ensure that the Department's information security initiatives are coordinated and managed effectively, and that the necessary progress is made towards attainment of the Department's information security objectives.

- Provides expert advice to senior management on the development, implementation, and maintenance of an information security infrastructure.

- Responsible for developing appropriate training and information security awareness initiatives essential to ensure policy compliance across the organisation.

- Reports on the key issues to be addressed at Departmental level in order to attain HPC's corporate objectives for information security, and with the guidance of the HPC member with functional responsibility for information security leads action to address those issues.

- Advises and assists the HPC member with functional responsibility for information security, and other HPC members as required, in scrutinising and challenging the Business Units on their progress towards attainment of the Department's corporate objectives for information security, and identifying action plans to address shortfalls as require

- Carries out research into, and advises on and assists implementation of, appropriate technology solutions and innovative information security management techniques to safeguard the organisation's assets, including intellectual property.

- Develops relationships with high-level law enforcement and intelligence agencies, other related government Departments and private sector bodies, in assessing and managing risks to information security.

- Manages information security incidents planning and investigation of security breaches, and assists with disciplinary and legal matters associated with such breaches as necessary.

- Provides regularly reports and relevant metrics on the status of information security across HPC

- Build a framework of compliance checking (including self assessment and Internal Audit) to ensure ongoing compliance with policy and standards.

- Responsible for maintaining and testing IT business continuity plans and the effective processes to enable the availability of information systems.

Key Skills, Competencies & Experience

- Leadership skills to provide direction to the management and professional staff within the organisation.

- Skills in strategic thinking with the ability to influence the Department's strategies so as to attain the Department's corporate objectives for information security.

- Ability to analyse and use evidence effectively to inform decision-making about information security being skilled in information security risk assessment and management.

- Financial management skills in making effective use of the Department's resources and assets, including development of clear business cases for investments to improve information security.

- Ability to apply people management skills effectively, in particular in the management of change and development of consensus in an organisational context where there are diverse operational activities.

- Advanced programme and project management skills, including the ability to define and lead cohesive programmes of action across HPC as a whole that are well-coordinated and make good use of the Department's overall resources.

- Ability to communicate information security policies and requirements clearly to all key audiences across HPC and to service providers.

- The ability to understand IT threats, vulnerabilities and specific related IT risks related to the effective control of IT across HPC.

- Broad understanding of information management and advanced expertise in information security.

- Expertise in business continuity planning, auditing, and risk management, as well as contract and vendor negotiation.

- Broad understanding of the businesses of HPC and the ability to define information security strategies, policies and procedures that are appropriate to their business setting.

- A clear understanding of standards relating to information security, such as ISO27000, CobiT, and or the ISF standards of good practice.

Qualification Guidelines

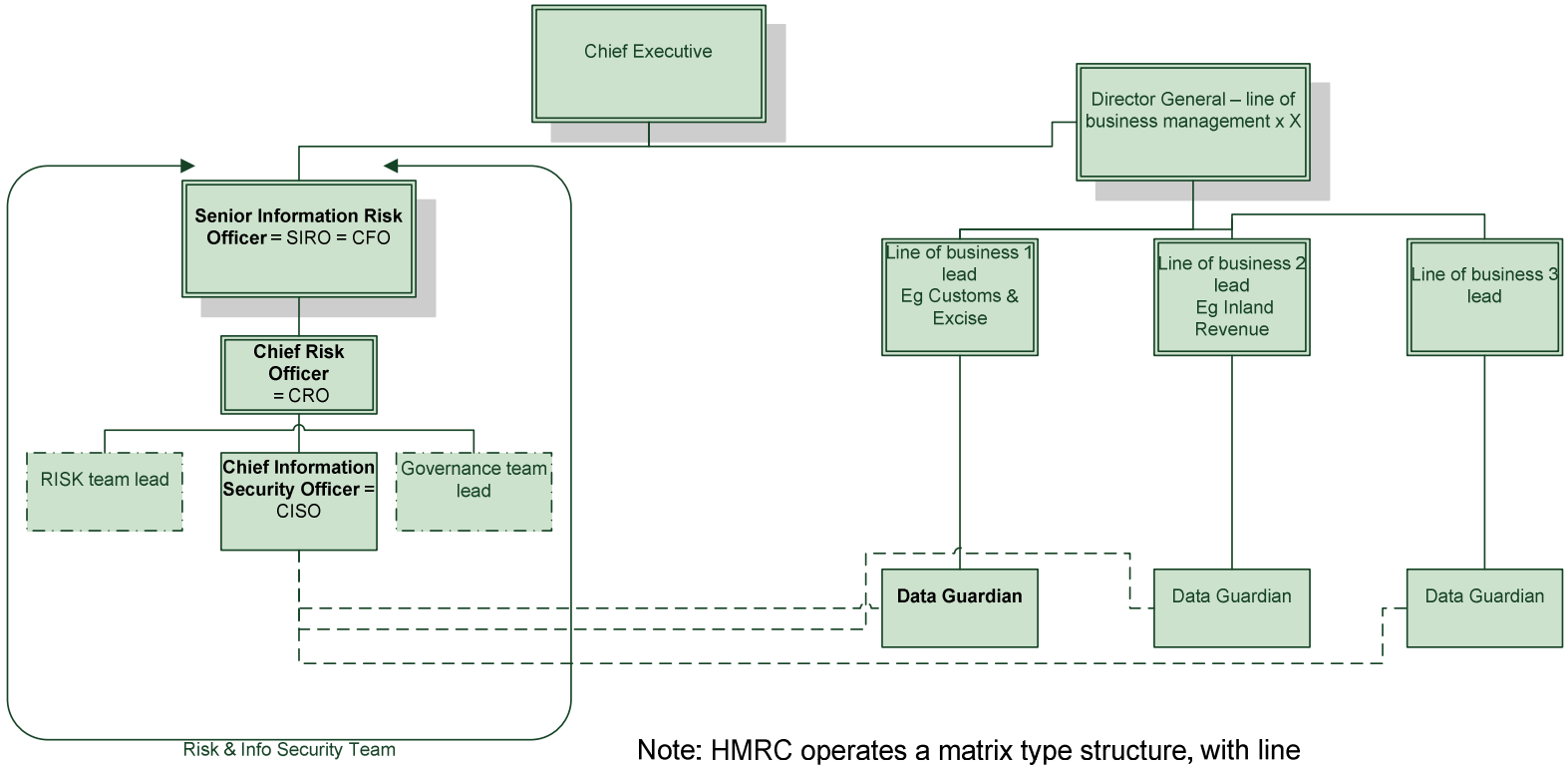
• At least 5 years of direct experience in a significant leadership role. Demonstrated ability to develop and manage the functional capital and expense budget.

• Advanced degree or equivalent in an area of study relevant to this position and at least 10 years of experience in a public or private sector corporate information security function.

Desirable to have a formal qualification in Information Security Management, and or membership to the institute of information security professionals (IISP) or Information systems Security Association (ISSA).

APPENDIX 3 HMRC Reporting structure for Information Risk

HMRC Reporting structure for Information Risk post Poynter Review 2008



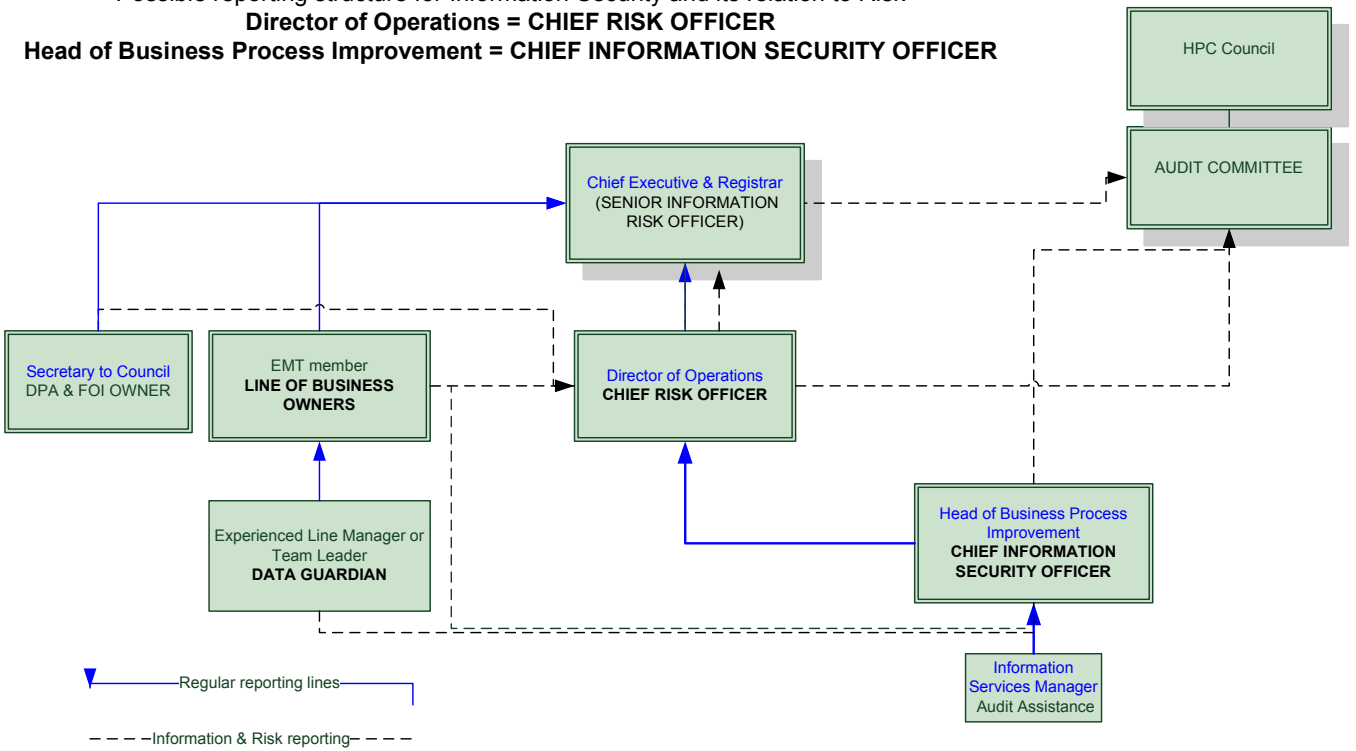
Note: HMRC operates a matrix type structure, with line of business elements including a Data Guardian, that works with the Information Security Team.
The Information Security and Risk functions work across the different lines of business and report (indirectly) to the Chief Executive.

APPENDIX 4 HPC's Proposed reporting structure based on HRMC post Poynter

Possible reporting structure for Information Security and its relation to Risk

Director of Operations = CHIEF RISK OFFICER

Head of Business Process Improvement = CHIEF INFORMATION SECURITY OFFICER



Roles required:	HPC equivalent	Poynter review role
	RISK OWNER,	= **CHIEF RISK OFFICER**
	INFORMATION SECURITY OWNER,	= **CHIEF INFORMATION SECURITY OFFICER**
	DATA GUARDIAN,	= **Data Guardian**

The role of Senior Information Risk Owner may well be excessive for an organisation of HPC's size.

Data management & information security at HPC – an overview

Roy P Dunn – Business Process Improvement and Information Security

Greg Ross-Sampson – Operations Directorate

9th December 2009

Content

- What is the state of the current information landscape?
  - What the Information Commissioner thinks is happening
  - Recent data loss incidents
- Where is HPC's data?
- An abundance of guidance from government
- Point by point response to the Poynter Review
- Risk & how we will manage Information Security at HPC
  - ISO27001/2
  - (Sample of training material if time allows)

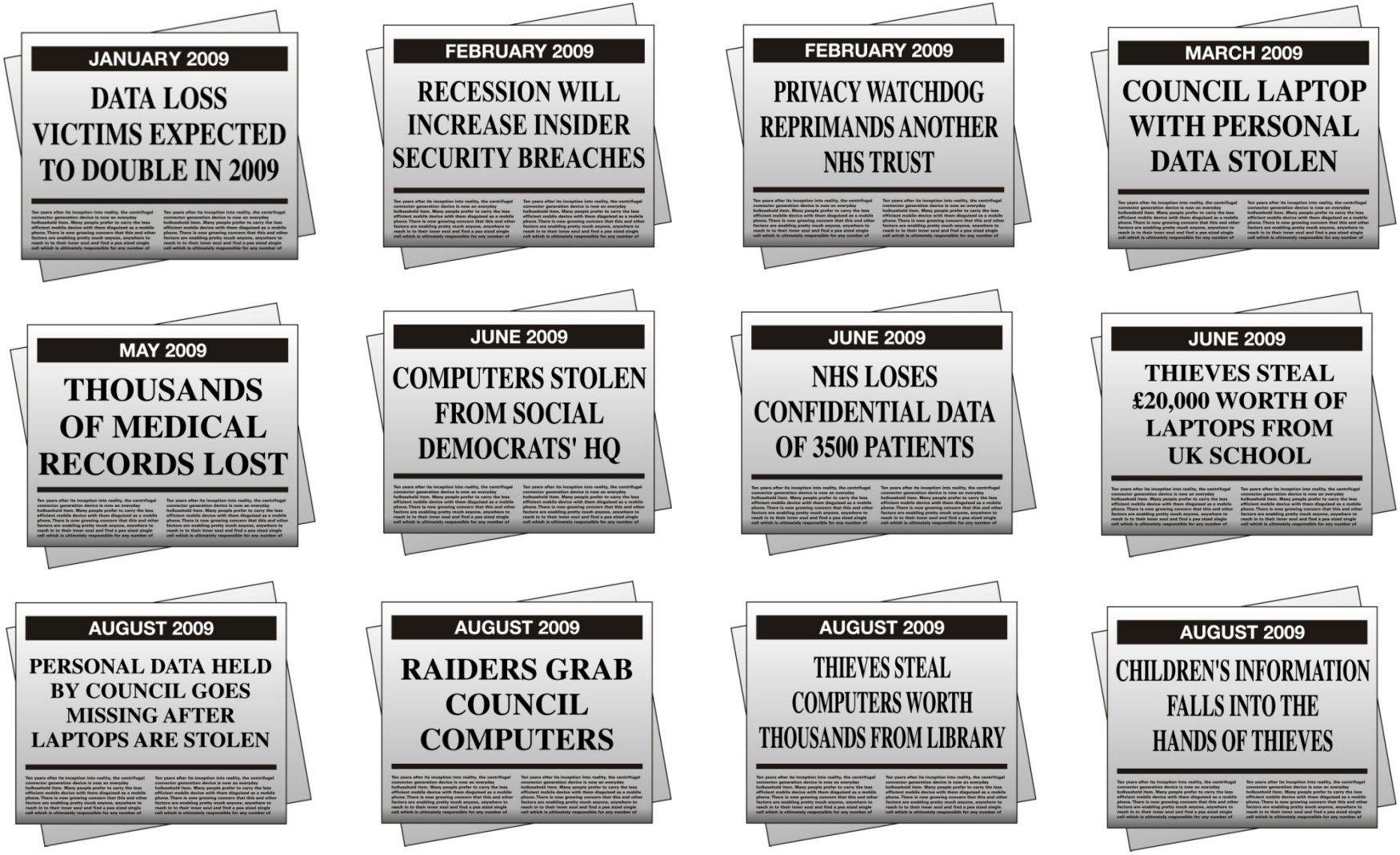
What is the state of the current information landscape?

The view from the Information Commissioners Office - Data Protection Officers Conference 4th March 2009

World's largest Data breaches – a snapshot

Numbers of people /records affected	Date on Incident	Organisation/Location
130,000,000	Jan 20th 2009	Heartland Payment Systems (US)
94,000,000	Jan 17th 2007	TJX Companies (US)
40,000,000	June 19th 2005	Visa, CardSystems, MasterCard, American Express (US)
30,000,000	June 24th 2004	America Online (US)
26,500,000	May 22nd 2006	U.S. Department of Veteran Affairs (US)
26,000,000	Nov 20th 2007	HM Customs and Revenue (UK)
8,637,405	March 12th 2007	Dai Nippon Printing Company (Japan)
8,500,000	July 3rd 2007	Fidelity National Information Services (US)
6,300,000	Sept 14th 2007	TD Ameritrade (US)
6,000,000	May 2008	Chilean Government (Chile)
5,000,000	March 6th 2003	Data Processors International (US)

Data Loss in the News – recent examples in the UK



Information loss in November 2009

Information loss in November 2009

METRO – London edition. Voters' details on stolen computer
Tuesday, November 17, 2009

- A laptop computer containing personal data on more than 14,000 voters has gone missing
- On the laptop were the names, addresses, dates of birth, signatures and copies of scanned postal vote application forms and postal vote statements used to confirm the identity of 14,673 voters.

This information is similar to that held by HPC

Tuesday, November 17, 2009 METRO 5

t:
rt

Remand: Delroy Grant is led away after the short court hearing, pending further charges
Picture: PA

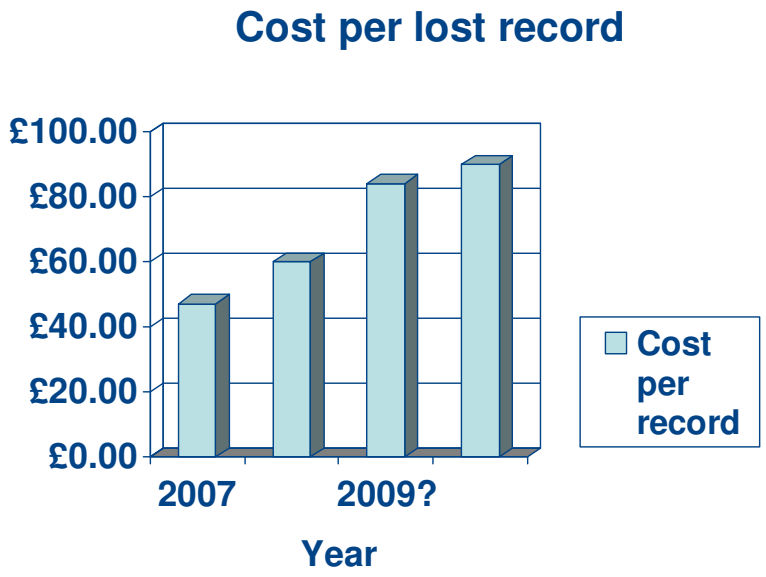
he lived with his
is confined to a
g struck down by
veral years ago.
the couple were
ah's Witnesses.

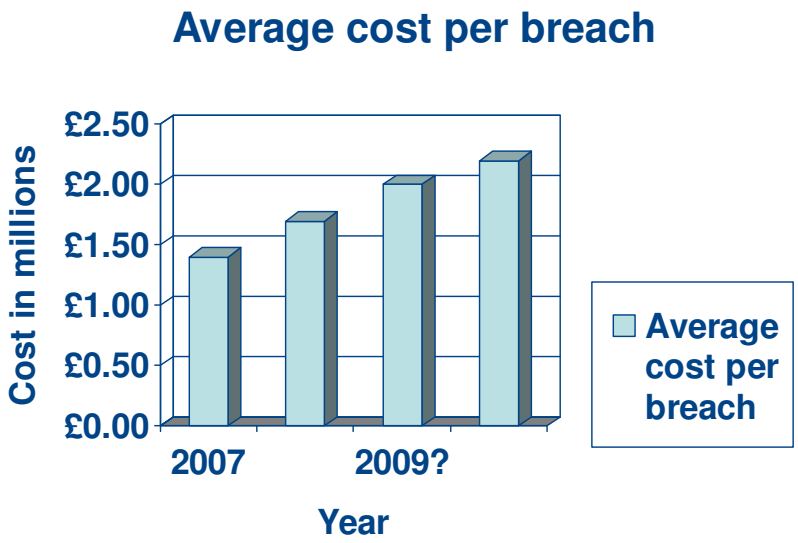
Data theft is 'perfect for fraud'

A LAPTOP containing personal data on more than 14,000 voters has been stolen from a local authority. It contained the names, addresses, dates of birth, signatures and copies of scanned postal vote application forms and postal vote statements used to confirm the identity of 14,673 people in June this year. The computer went missing from the offices of St Albans City Council in an opportunistic theft. 'That's all the information you need to set up a bank account,' said councillor Julian Daly. 'It's perfect identity theft territory.' The council says there is 'a slight risk' a criminal could access the data and is writing to everyone affected.

early

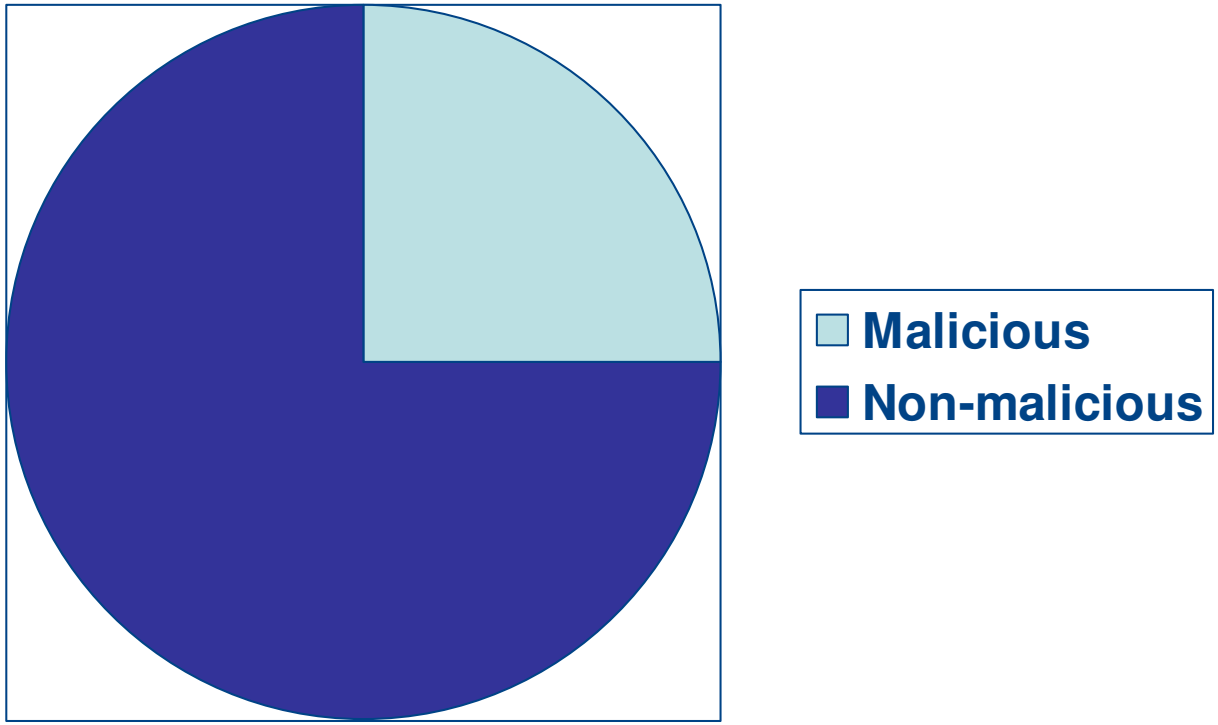
Costs associated with data breaches - Ponemon Institute report 2008





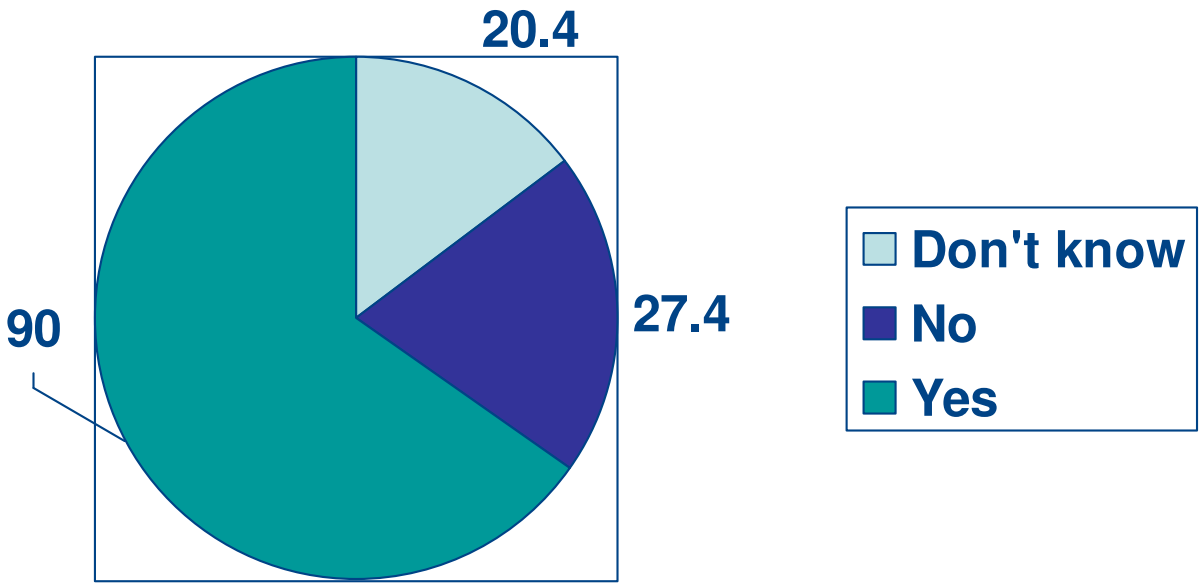
The Information Commissioners' Office is consulting on a maximum fine level of £500,000 per breach, having had no powers to fine to date.

Causes of Data breaches – IDC 2009



IDC statistics on PC/laptop theft or loss and background.

Has your organisation experienced PC/laptop theft or loss?



The latest phishing scam……..

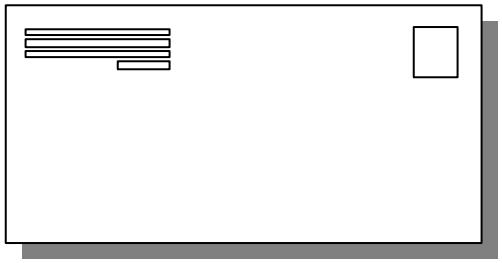
- In October 2009, persons were receiving telephone calls from the ‘Police’….. “Good Afternoon Sir, your name has been given by a person we have stopped in the street, as someone that can confirm their identity. Before I asked you to do that, can you confirm your identity please, so we can make sure we know who we are talking to…And your address and date of birth…..”

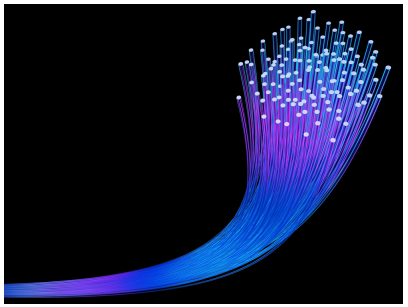
- The callers just steal the call recipients details.

Where is HPC's data

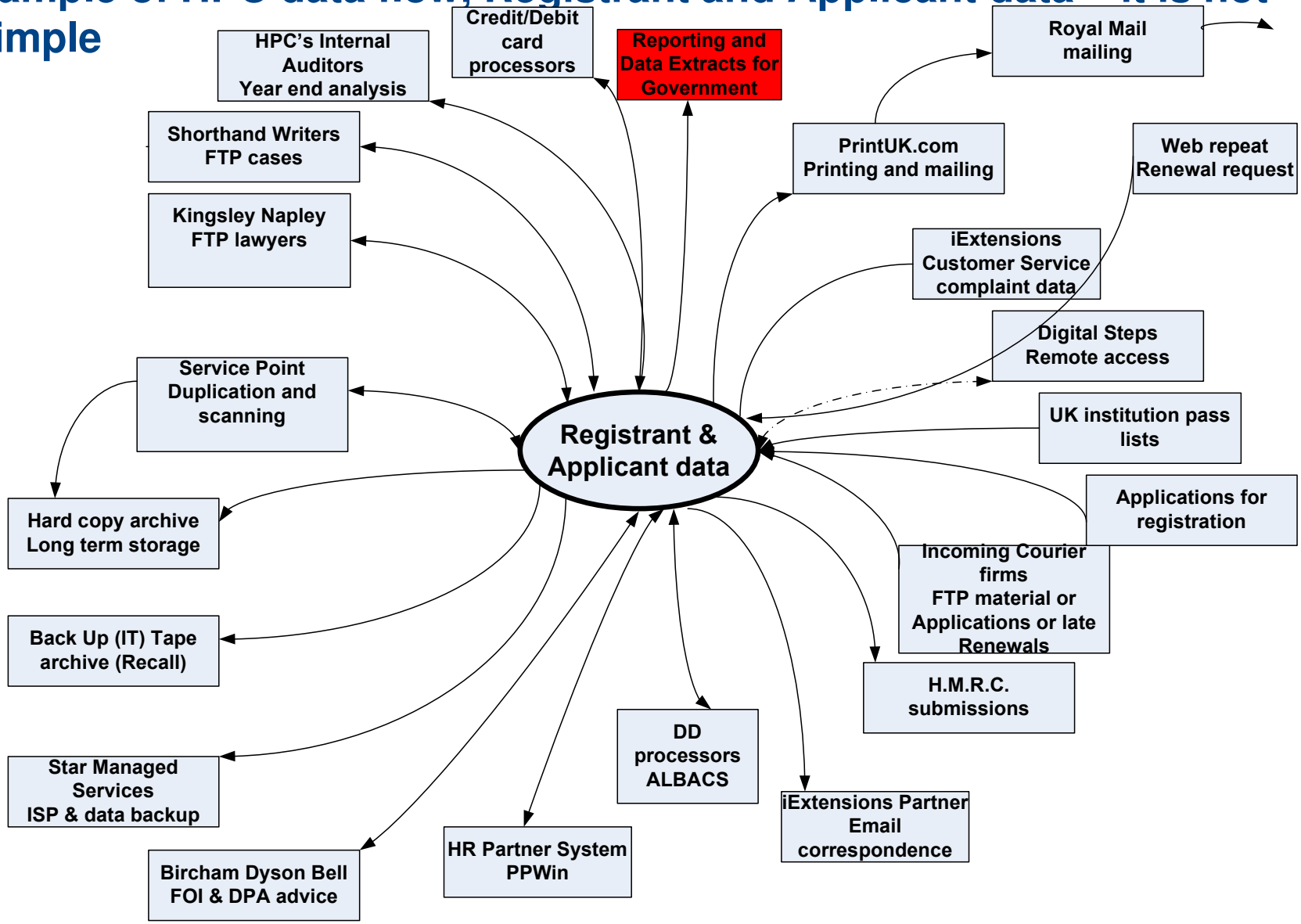
Where is information used at HPC?

How is information stored or transmitted at HPC?

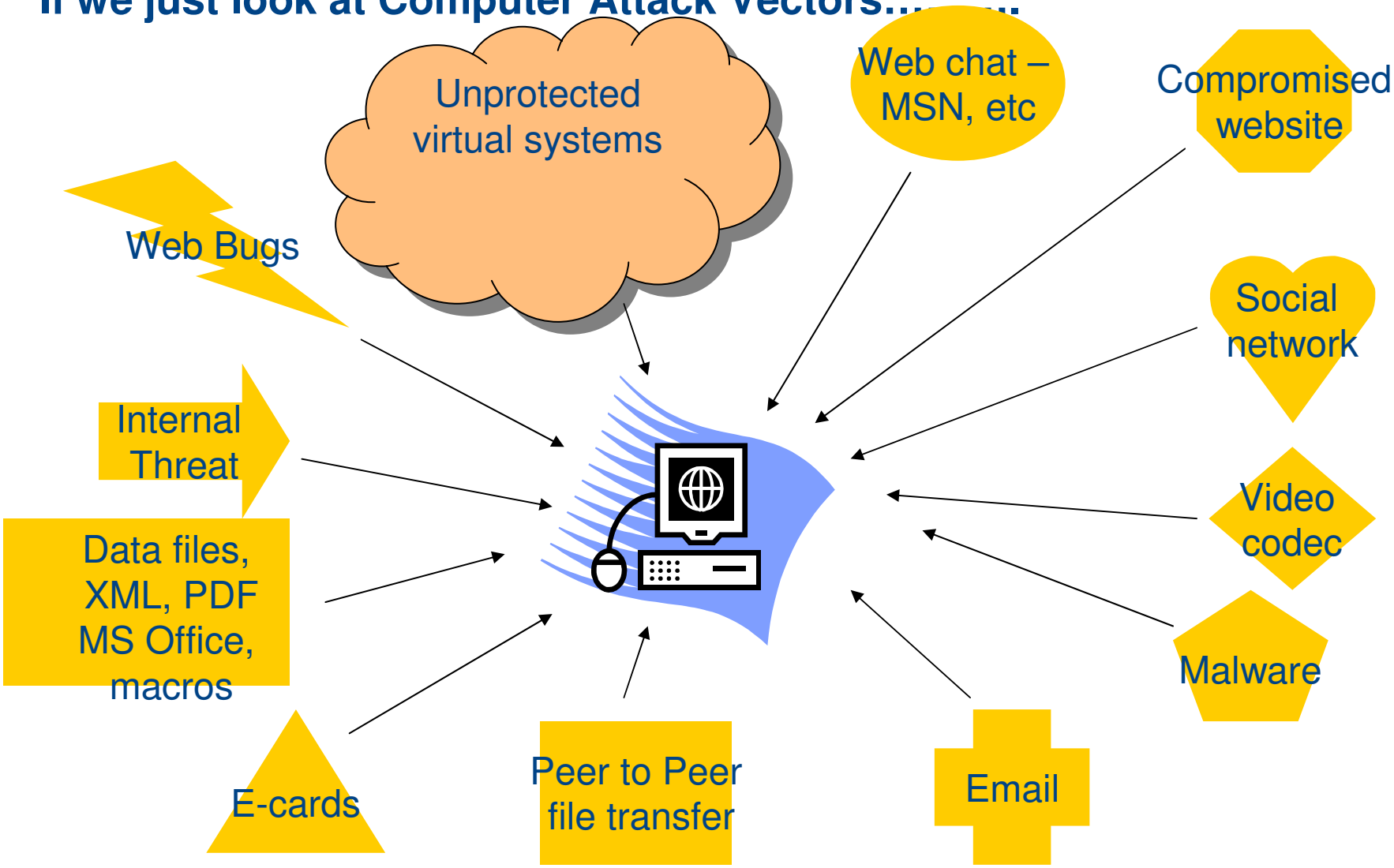




Sample of HPC data flow, Registrant and Applicant data – it is not simple



If we just look at Computer Attack Vectors……



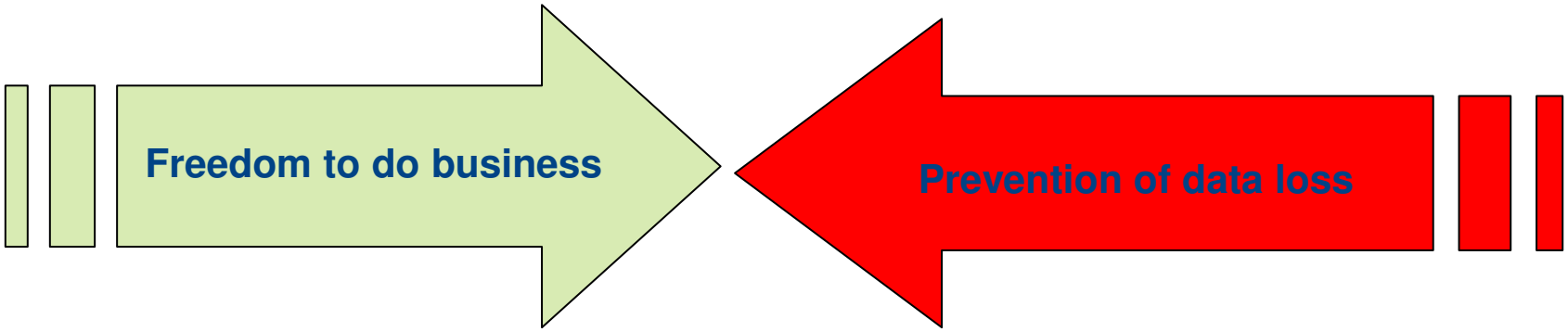
An abundance of guidance from government

An abundance of guidance from government

HMG Guidance on the matter is growing..

- Cabinet Office - Central Sponsor for Information Assurance: A National Information Assurance Strategy
- Cabinet Office - Protecting Government Information: Independent Review of Government Information Assurance - The Coleman Report (June 2008)
- Cabinet Office - Data Handling Review: Cross Government Actions: Mandatory Minimum Measures
- Cabinet Office - Data Handling Procedures in Government: Final Report (June 2008)
- Cabinet Office - Data Handling Procedures in Government: Interim Progress Report (December 2007)
- Cabinet Office - Security: e-Government Strategy Framework Policy and Guidelines Version 4.0 (September 2002)
- Cabinet Office - Hannigan Recommendations (2008)
- Cabinet Office - HMG Security Policy Framework Version 1.0 (December 2008)
- Cabinet Office - National Risk Register (2008)
- Cabinet Office - The National Security Strategy of the United Kingdom: Security in an interdependent world (March 2008)
- Deloitte - 2007 Global Security Survey: The shifting security paradigm
- Department for Business Enterprise & Regulatory Reform - Regulators' Compliance Code: Statutory Code of Practice for Regulators (17 December 2007)
- Department for Business Enterprise & Regulatory Reform - 2008 Information Security Breaches Survey: Executive Summary
- Department for Business Enterprise & Regulatory Reform - 2008 Information Security Breaches Survey: Technical report
- Department of Health - Information governance in the Department of Health and the NHS, Harry Cayton, National Director for Patients and the Public, Chair, Care Record Development Board (September 2006)
- Department of Health - Information Security Management: NHS Code of Practice (April 2007)
- European Commission - Proposal for a Directive of the European Parliament and of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic

Information Security Management is a constant balancing act, between the needs of the organisation to do business, and attempting to prevent accidental or deliberate data leakage.



Data management & information security at HPC

HPC's approach to Data Management & information security

- Management responsibility
- ISO9001
- HPC Risk register
- Analysis of incidents

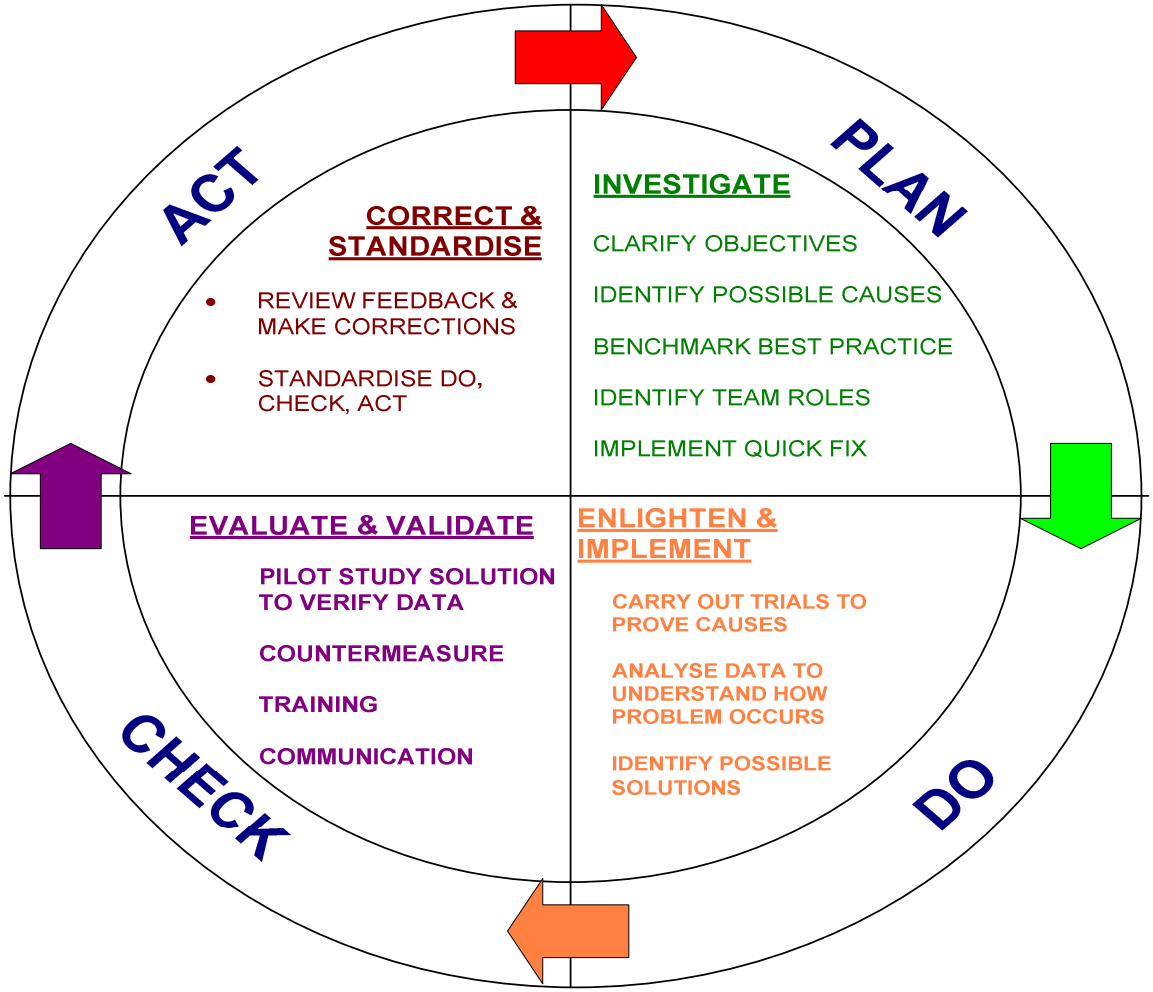
Management Responsibility

- All employees are required to treat information securely;
    - This is indicated in job descriptions and contracts
    - And access to data is restricted on a need to know basis
    - The ability to carry out bulk data extraction is very limited
    - Requirement for security is reinforced in training to the whole organisation

Example of all company training

ISO 9001:2008 Plan – Do – Check – Act continuously checks controls

Audit current controls and records



HPC risk register.

HPC RISK MATRIX

Catastrophic 5	5	10	15	20	25
Significant 4	4	8	12	16	20
Moderate 3	3	6	9	12	15
Minor 2	2	4	6	8	10
Insignificant 1	1	2	3	4	5
IMPACT / LIKELIHOOD	Negligible 1	Rare 2	Unlikely 3	Possible 4	Probable 5

Key		
	>11	High Risk: Urgent action required
	6 - 10	Medium Risk: Some action required
	<5	Low Risk: ongoing monitoring required

HPC Risk Register September 2009

Data Security

Ref	Category	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations September 2009	Likelihood before mitigations September 2009	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation September 2009	RISK score after Mitigation February 2009
17	**Data Security**	17.1	Electronic data is removed inappropriately by an employee	Director of IT	5	3	15	Employment contract includes Data Protection and Confidentiality Agreement	Adequate access control procedures maintained. System audit trails.	Laptop encryption. Remote access to our infrastructure using a VPN . Documented file encryption procedure	Low	Low
			Links to 5.3									
		17.2	Paper record Data Security	Head of Business Improvement	5	3	15	Use of locked document destruction bins in each dept. Use of shredder machines for confidential record destruction in some depts e.g. Finance.	Data Protection agreements signed by the relevant suppliers. Dept files stored onsite in locked cabinets.	Regarding Reg Appln forms processing, employment contract includes Data Protection Agreement	Low	Low
			Links to 15.7									
		17.3	Loss of electronic data held by third party suppliers in the delivery of their services	Director of IT	5	3	15	Data Protection/Controller agreements signed by the relevant suppliers. Use of electronic firewalls by suppliers.	Data transfer using file level encryption. Physical transfer of back up tapes using specialist company with locked boxes and sign out procedure.	Remote access to our infrastructure using a VPN. Access to third party infrastructure using agreed secure methods.	Low	Low
		17.4	Data received from third parties	Director of Ops, and Director of FTP	5	2	10	Read only, password protected access by a restricted no of FTP employees to electronic KN data.	Registrant payments taken in compliance with Payment Card Industry (PCI) Security standards ie with quarterly PCI testing.	Ensure third party data providers e.g. professional bodies provide the data password protected/encrypted/door to door courier/registered mail/sign in sign out as appropriate.	Low	Low
		17.5	Loss of physical data despatched to and held by third parties for the delivery of their services	Director of Ops and Hd of Business Process Improv	5	3	15	Data Protection/Controller agreements signed by the relevant suppliers. Use of electronic firewalls by suppliers.	Use of transit cases for archive boxes sent for scanning or copying and sign out procedures.		Low	Low

However, at anytime Risk owners think they are managing risk – but do not always get it right. - Proper risk management must drive security

"Never in all history have we harnessed such formidable technology. Every scientific advancement known to man has been incorporated into its design. The operational controls are sound and foolproof!"

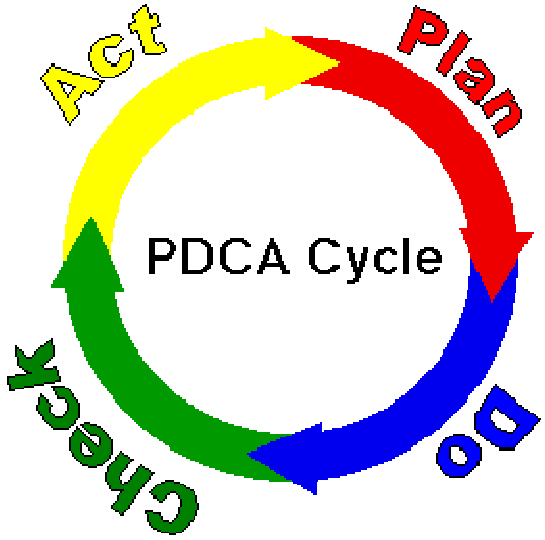
E.J. Smith, Captain of the Titanic

Analysis of incidents or external reports that could influence HPC

Past Analysis of incidents or external reports that could influence HPC

Eg

HMRC cd loss report to Council & Committees Dec 2007
NMC CHRE review May 2008
Break in at HPC summer 2009
Poynter Review into HMRC data loss June 2008 reported to Audit Committee Dec 2009
GSCC CHRE review 2009 (in preparation)



Point by point response to the Poynter Review

What is the "*Response to the Poynter Review and Cross Government Actions: Mandatory Minimum Measures*" report?

- In November 2007 HMRC lost 26,000,000 records of family members, including children after sending an unencrypted pair of CD's through the internal mail system. This loss resulted in the review by **Kieran Poynter**, covering how the data loss occurred, and how similar events could be prevented in future. The review ranged from the requirement to share data, through to IT strategy. It mandates a move away from paper exchange of information to online channels, and strongly suggests adoption of ISO27001 as an information security standard.
- HPC has used this report "**Review of information security at HM Revenue and Customs -** Final report" by **Kieran Poynter** as a basis for audit in the document "Response to the Poynter Review and Cross Government Actions: Mandatory Minimum Measures" of which this presentation is a summary

Poynter Recommendations R1 - R4

Recommendation or Issue number	Issue area	Primary responder	Secondary responder	Possible deliverables and timescales where suggested
R1	Information security as a Corporate objective reflected in mission and strategy	Marc Seale		Information security is included as an ongoing organisational goal in high level EMT (Council?) documentation. By July 2010 The responsibilities of a "Chief Information Security Officer" will be assign to an existing individual at HPC
R2	Line of business objectives around info security should support corporate objective of R1	Marc Seale		Department work plans refer to information security, supporting the Councils goal. (R1) ongoing. (all dept heads)
R3	Business & IT strategy should be updated to make them consistent with this (Poynter) report	Guy Gaskins	Marc Seale	Information Technology strategy Objective 3 already refers to secure and recoverable information assets and services. Infosecurity to be included in dept objectives in future.
R4	Policy & legislation should be updated to specify how customers interact with the organisation	Greg Ross-Sampson / Michael Guthrie?		Promote delivery of existing online systems in preference to paper based communications. Develop and promote further online services. Consider possible legislative change to offer online exclusively at some stage in the future?

Poynter Recommendations R5 – R9

R5	Formalise the Information Security strategy and ensure it supports the updated business and IT strategy	Guy Gaskins / Roy Dunn		Appointed CISO to develop an information security strategy across HPC. Roll out and audit against the associated policies. Suggested date January 2010 Examine HMRC approach plus timescales for delivering ISO27001 level controls, then achieving full externally audited compliance.
R6	Locate quick wins to kick start the information security direction of travel	Guy Gaskins / Roy Dunn		Basic data flows have been mapped. Encryption processes have been made available for all employees. Laptop encryption in place since 2004/5 Online renewal services are being developed, address changes are already online.
R7	Identify and investigate initiatives for the medium term	Guy Gaskins / Roy Dunn	Claire Reed	Secure paper storage is in place after scanning processes make information available electronically. Online services have been highlighted as an area for investment
R8	Achieve a better balance between strategic and tactical investment	Guy Gaskins	Marc Seale / Gary Butler?	Long term investment plans are in place, but some isolated systems will remain. Data exchange will be provided where possible / desirable.
R9	A Data security programme should coordinate and manage security activities and initiatives	Roy Dunn Greg Ross-Sampson		Upon appointment of CISO responsibilities, commence requirements capture and provisioning of training from November 2009

Poynter Recommendations R10 - R16

R10	Data security programme board should be sponsored by the Senior Information Risk Officer	Marc Seale		SIRO not used at HPC as makes organisation top heavy. (Info Security sponsored by Chief Exec & Chief Risk Officer anyway, so no added value in making an additional mgmt role)
R11	Appoint a Chief Risk Officer	Marc Seale		CRO position in place from June 2009 after EMT discussion. Greg Ross-Sampson appointed by EMT.
R12	Appoint a Chief Information Security Officer	Marc Seale	Greg Ross-Sampson	Decision to be made on where this responsibility will be held in HPC. By October 2009 CISO role suggested for Head of Business Process Improvement as already reports to holder of CRO position/role.
R13	Establish a professional risk management function in the lines of business	Marc Seale	Greg Ross-Sampson	Risk Management enhanced in February 2009. Located in Operations Directorate, (Director of Operations) with day to day activity by Business Process Improvement. CRO position / role incorporated into existing role.
R14	Chairman, Chief Executive and COO and advisors should periodically challenge the line of business on Information security	Marc Seale	Roy Dunn	Chief Executive and EMT members will discuss information security and related business issues at 1-1's Chief Executive and EMT/CDT will evaluate any new information security risks, and plan and implement a response.
R15	Engage staff by communication and avoid scepticism	Jacqueline Ladds		Develop long term info security education & communication plan for whole organisation. Commence planning March 2010. Input from CISO position upon requirements.
R16	Coordinate HR, Communications Learning and change activities to ensure Info Security policy and process are embedded in everyday behaviour	Jacqueline Ladds / Teresa Haskins	Roy Dunn	Infosecurity already discussed at a number of internal forums and inductions. Investigating online info security training resources.

Poynter Recommendations R17 - R21

R17	Ensure staff at all levels understand their responsibilities and apply policies and principles	COMMS / Business Process IImprov?	HR Manager	Enhance employee induction process to include Information Security training at earliest possible opportunity. Keep internal documents short to medium length to ease understanding. Assign a local lead in each department.
R18	Incorporate info security messages and controls from recruitment to leaving the organisation	Teresa Haskins	Roy Dunn	Pre-employment and pre exit procedures are in place. Contractual terms reference information security, intellectual property rights and confidentiality.
R19	Develop and implement Info Security awareness prog & refresher trng	Jacqueline Ladds / Teresa Haskins	Roy Dunn	CISO position to design and test deliver initial Info Security training programme. By end March 2010
R20	Build appropriate levels of capability in Mgmt of Information security across the organisation	Greg Ross-Sampson		Decision required on Senior Risk Officer / Chief Risk Officer / Chief Information Security Officer / Data Guardians by October 2009. (No SIRO, CRO decided June 2009. just CISO & DG roles to be confirmed) Appropriate training to be undertaken within two years?
R21	How to drive change within the organisation	Marc Seale? / Teresa Haskins	Roy Dunn	Need to decide on way to implement info security around HPC, and involving it in all ongoing team, project and planning processes. Clear desk working for areas with confidential information. By end December 2009 Non functional specifications to include infosecurity for all projects.

Poynter Recommendations R22 – R27

R22	Information security policy should be simplified, shortened and made more accessible.	Roy Dunn / Guy Gaskins	Jacqueline Ladds	Readable, brief security policy applicable to whole organisation rolled out by December 2009 (Electronic records policy to be developed in near future.)
R23	Information security policy should be translated for all business units and made applicable for local procedures and accountabilities made clear.	Roy Dunn / Any EMT		HPC will aim to implement the activities and policies to achieve ISO 27001 Information Security Standard; and BCS Information Security Management Principles (CISMP) by October 2010, subsequently attempting certification by October 2011
R24	Take a more proactive stance on incident management	Roy Dunn		Develop central reporting function for info security issues within HPC, carrying out route cause analysis where applicable. By end December 2009 Monitor info security forums, attend appropriate meetings to remain alert to potential new threats.
R25	Adopt a more structured approach to auditing adherence to information security	Roy Dunn / Greg Ross-Sampson		Adopt ISO 27001 and CISMP as examples of best practice. EMT members to maintain oversight of info security in their lines of business. Look to implement the activities and policies to achieve ISO 27001 Information Security Standard; and BCS Information Security Management Principles (CISMP) by October 2010, subsequently attempting certification by October 2011
R26	Lines of business should identify a security sponsor and appoint an info security professional	Any EMT / Greg Ross-Sampson	Roy Dunn	EMT have line management for information security in their lines of business. Data Guardians will be assigned in each line of business, to help in evaluation of day to day info security issues. By End February 2010
R27	Lines of business should identify a risk sponsor and appoint a risk professional	Marc Seale	Roy Dunn / Greg Ross-Sampson	HPC will assign Risk to the Director of Operations area, with day to day input from the Business Process Improvement team. Line of business risk will be monitored by the appropriate EMT members. Also see Appendix 1 Accountabilities & Responsibilities mapped to HPC

Poynter Recommendations R28 – R33

R28	Ensure that data exchanges between business units and shared resources are secure (CRM paper)	Roy Dunn		RPD to write paper evaluating options for single customer record / customer relationship management within HPC; maximising data security and minimising re-keying of data where possible. (February 2010)
R29	Data guardian and info security professionals within the business should include "people" responsibility	Roy Dunn	Greg Ross-Sampson/Marc Seale	CISO to develop role description for Data Guardian, and develop training requirements. DG roles will be added to existing employees functions. EMT retain line of business responsibility. By end February 2010
R30	Lines of business should be "accountable" for mail handling on their behalf (this is not suggesting FTP process their own post etc)	Steve Hall?	Richard Houghton / Gary Butler / Kelly Johnson	Implement sign off processes for collection / delivery of sensitive mail. Single mail room to be retained. Some lockable overnight post box type storage to be purchased for sensitive areas of the business.
R31	Access control should be consistent across all systems and estate	Guy Gaskins	Roy Dunn	Multi level sign on required to access systems with sensitive data. An audit of existing IT access controls against policy will be commencing December 2009 Building controls for the separation of the HPC campus into public and confidential areas to be implemented before Xmas 2009
R32	All business units should review capacity requirements for current and future paper storage – ensuring compliance with the clear desk policy	Roy Dunn	Steve Rayner Kelly Johnson	Desk storage only allowed for non confidential information. Lockable storage for all other items required. Scan link and destroy hard copy where possible. Move to electronic/networked storage where possible integrated with online delivery systems.
R33	Map end to end data flows at the right level of detail to enable enforcement of info security risk identification	Roy Dunn		Basic level mapping completed. Use these and QMS processes to determine where infosecurity issues could develop. Need to reflect ongoing changes to what is considered best practice. (eg PCI DSS)

Poynter Recommendations R34 – R38

R34	Service level agreements (SLA's) should be agreed to ensure service meets business requirements	Guy Gaskins / Roy Dunn		SLA's to be reviewed with IT suppliers over the current financial year. Data exchange policies to be formalised.
R35	Initiate a programme of third party information security assurance	Roy Dunn	Greg Ross-Sampson	Monitor suppliers / partners adherence to ISO 9001:2008 or information security standards (ISO27001 or others), and encourage adherence to similar standards for ongoing supplier relationship. Where no certifications are held by suppliers consider auditing those parties ourselves.
R36	Project approval should include ensuring business owners understand the (info security) risks they are being asked to accept	Claire Reed	Greg Ross-Sampson Any EMT	Ensure documentation for individual projects highlights information security risks at operational and storage levels. Changes or enhancements to IT systems and paper processes should increase security and decrease risk.
R37	Evaluate contracts with suppliers to ensure adequate information security	Secretariat (Colin Bendall)	Gary Butler	ASPIRE is an outsourcing contract held by HMRC. HPC do not have data processing or IT outsourcing contracts in place. Therefore data transfer not required. Additional note: 14/09/09 Potentially move away from suppliers unwilling to allow either contractual information security or information security compliance audit.
R38	Create strategy for the replacement of legacy systems, including the possible adaptation of existing systems for other work	Guy Gaskins		HPC does not use the Child Benefit System or have similar data sharing requirements. Addition of section to ongoing IT strategy for 2010-2011 Financial year. Determine if consolidation of data and IT storage and systems is required for an organisation of HPC's size and proposed complexity. (CRM paper)

Poynter Recommendations R39 – R42

R39	**IT investment model should include greater risk quantification**	**Guy Gaskins**	**Claire Reed/Greg Ross-Sampson**	**Slight enhancement to all IT investment documentation for 2010-2011 onwards. Highlight Risk as input to the decision making process. £50k possible financial impact for a single hard copy data loss.(Benjamin James, Bircham Dyson Bell 2009)**
R40	**Strengthen business requirement specification particularly around non-functional requirements**	**Claire Reed**	**Guy Gaskins**	**Project Management and IT to develop standard non-function requirements for all future projects. By March 2010**
R41	**Business continuity management (Disaster Recovery) should be enhanced**	**Roy Dunn**		**Ensure change management processes update the requirements and capability of the HPC business continuity plans – ongoing.**
R42	**Recommendations on the new direction of travel.** **Move from Business Unit IT project commissioning to corporate project commissioning** **XIv.2 move from making minor changes to processes to improve security, to changing the processes significantly to improve effectiveness and security. Remove islands of information.** **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).	**Guy Gaskins**	**Claire Reed**	**EMT evaluate all proposals for major and minor project expenditure. Information security has the highest ranking for development.** **HPC will offer secure online access, multiple communication channels with the most secure highlighted and promoted. Data integrity will be enforced. CRM or SCV will be implemented if / where possible.**

Poynter Recommendations R43 – 45 plus Supplementary items

R43	Build the business case for the new direction of travel, including route map, timescales and investment required	Guy Gaskins	Roy Dunn / Claire Reed	HPC have published rolling 5 year IT strategies since 2004. Scalability, reliability and security have been key deliverables throughout. Major IT developments are pre-validated by our penetration testing company.
R44	Engage professional help to develop the direction of travel, route map and business case.	Guy Gaskins		HMRC action point only. Not required at HPC
R45	Enhance capabilities in Information Management systems dept to enable IT and the direction of travel	Guy Gaskins		HPC do not have the type of outsourcing agreements referred to in this item. Evaluate current IT capability against future requirements, and enhance provision if required by the business.
Supplementary items to be included in this review	Physical Security Archive	Steve Hall & Marc Seale Roy Dunn		Put improved levels of building security in place, with electronic access controls; breaking HPC campus into public and confidential areas. Potential HPC culture issue. Action commenced following office break in August 2009 By December 2009? Relocate paper storage to archive in more secure environment, implement ongoing audit process, and secure access controls to departmental level data.

Poynter Recommendations

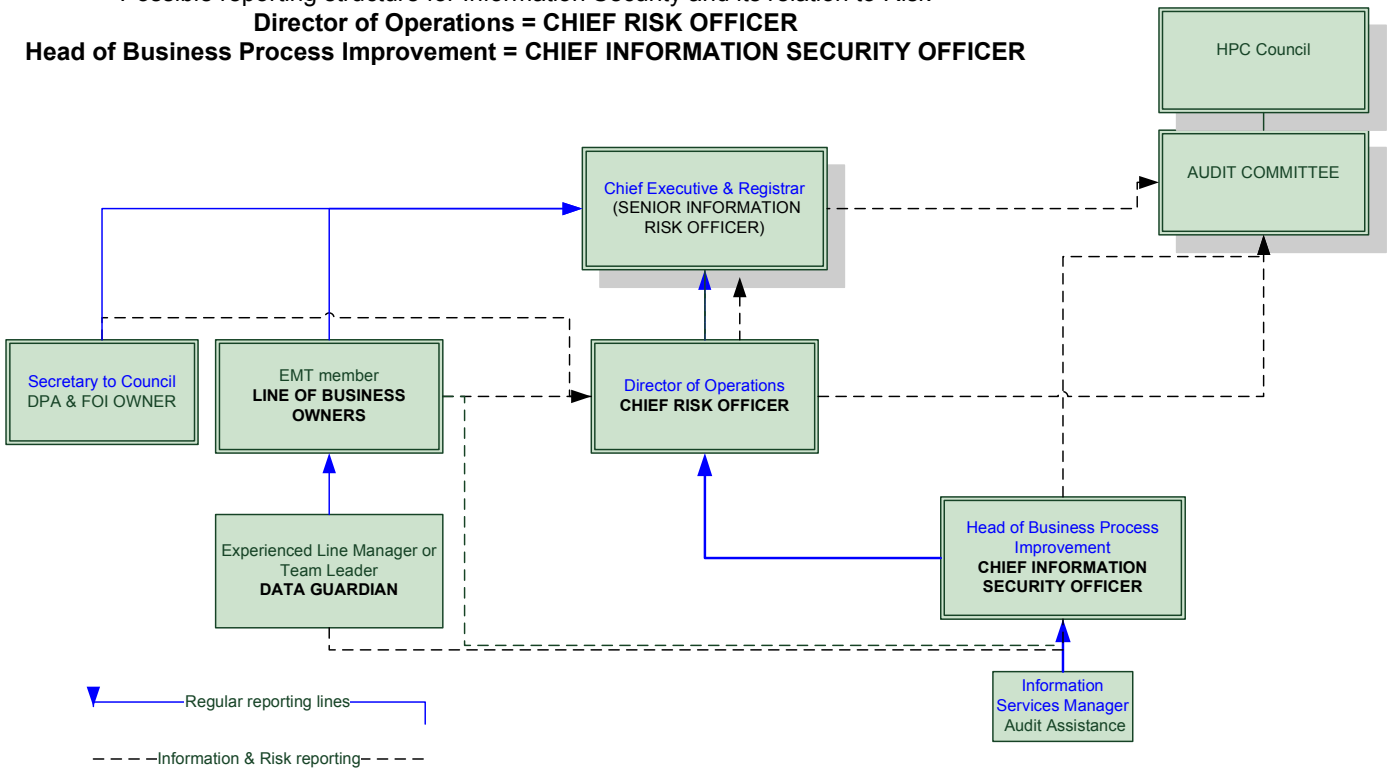
	Poynter's Ten Principles of Information Security	For Information Only		**Provides summary view of how information security should be organised based on the Poynter review.**
	Cross Government Actions: Mandatory Minimum Measures	For Information only		**Provides a Cabinet Office view of how information security should be organised.**
	Minimum scope of protected personal data	For Information only		**Classification and Identification of data held and used by HPC (Also covered in the Information Asset policy)**
Appendix 1	**Accountabilities & Responsibilities mapped to HPC**	**Marc Seale & any EMT**		**Determine if the Poynter responsibilities for each area described are appropriate, by October 2009 Mapped item by item to HPC.**
Appendix 2	**Chief Information Security Officer job description based on PriceWaterhouse Coopers specification**	**Marc Seale Greg Ross-Sampson**		**Determine if the responsibilities for this area (CISO) are to be held by a named individual, by October 2009.**
Appendix 3	**HRMC Reporting structure for information Risk post Poynter Review**	**Any EMT**		**For information only. Ideal information security structure at HMRC 2009**
Appendix 4	**HPC's proposed reporting structure based HRMC post Poynter**	**Any EMT**		**Agree / modify proposed HPC information security structure, by October 2009**

How HPC are going to operate Information Security

Possible reporting structure for Information Security and its relation to Risk

Director of Operations = CHIEF RISK OFFICER

Head of Business Process Improvement = CHIEF INFORMATION SECURITY OFFICER



Roles required:	HPC equivalent	Poynter review role
	RISK OWNER,	= **CHIEF RISK OFFICER**
	INFORMATION SECURITY OWNER,	= **CHIEF INFORMATION SECURITY OFFICER**
	DATA GUARDIAN,	= **Data Guardian**

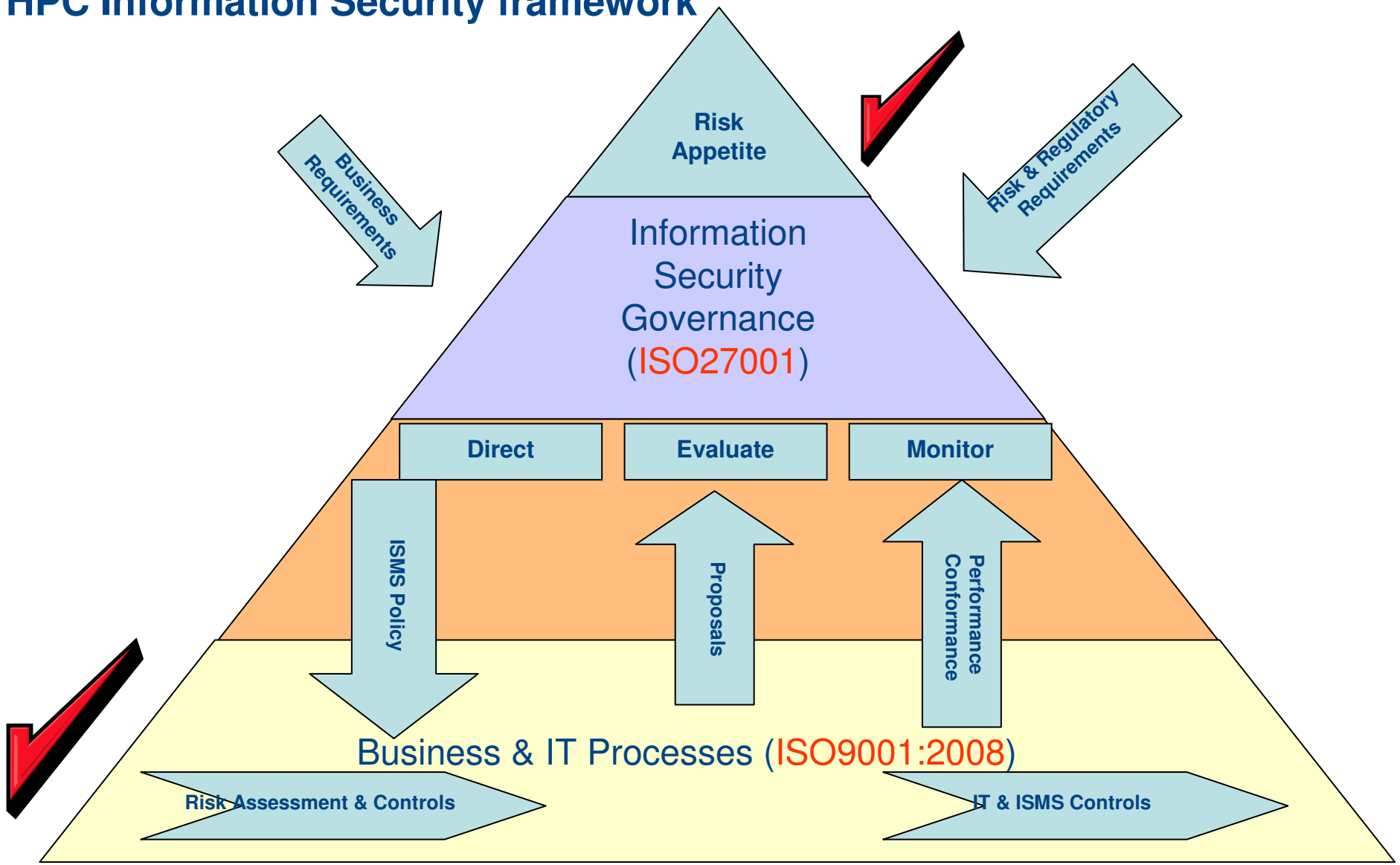
The role of Senior Information Risk Owner may well be excessive for an organisation of HPC's size.

Risk & how we will manage Information Security at HPC
ISO27001/2

ISO 27001 benefits

- ISO 27001 is "the umbrella for information security managers." It cuts across all security-related operations to bring a sense of formality and explicit management to controls, ensuring you don't overlook any aspect of security. Those adopting ISO 27001 are subjected to audit and must be continuously compliant to maintain certification.

HPC Information Security framework



ISO 27000 series of standards cover the following areas – it is not just about IT

- Data Security
- Data storage protection
- Data processing
- Computers
- Management
- Computer networks
- Computer hardware
- Computer software
- Data transmission
- Information exchange
- Access

Sample of Information Security training at HPC

- Barclays Bank plc worldwide training DVD has been shared with other organisations, as long as Copyright / Performing Rights considerations are taken into account in its use.