Protecting Government Information

Independent Review of Government Information Assurance

The Coleman Report

Commissioned by the Cabinet Office

June 2008

Contents

Annexes

Preface

In this review of how government handles and protects the information it holds, I have focussed on all elements of Information Assurance – data protection, availability and the integrity of information. I have considered departments and agencies across government and looked at these and other areas of the public sector to be able to form a view as to how well government overall is doing in Information Assurance.

This Independent Review was started before the announcement of the Cabinet Secretary's review of data handling and the bulk of the research for this report was completed in 2007. The Cabinet Secretary and his review team have sought my advice and used my review in the completion of their work. I welcome the conclusions of the Cabinet Secretary's review and look forward to seeing how they are implemented in government.

Where appropriate my report has been updated to reflect changes which have been announced as part of the Data Handling Review.

The findings and recommendations in my review have been drawn from a number of sources including interviews with stakeholders, attendance at committees and working groups, a partial survey and discussions with representatives from government departments. This work has been undertaken over 18 months and was completed in March 2008.

The report is published to record the rationale behind my recommendations and provide substance for the discussion around public sector Information Assurance. The challenges identified are both short and long term and the Government will need to show continued commitment to address them.

A number of illustrations have been used to demonstrate my findings. These illustrations may become out of date over time – and should therefore only be seen as examples to demonstrate the findings and key challenges for government.

In completing this review the cooperation of departments, agencies and stakeholders in the public and private sectors has made this work possible. Their openness and responsiveness has been excellent and I am most grateful to them for their time and support.

Specific thanks go to my sponsors in the Cabinet Office and the Security Services. I would also like to thank my communications support team who have provided me with the ability to distil my work into a readable format. I hope that colleagues working in the public and private sectors will find this report useful.

Nick Coleman

Nick Coleman
Independent Reviewer

Information Assurance

As defined by government – The confidence that information systems will protect the information they handle and will function as they need to, under the control of legitimate users

Executive summary

Government is transforming the way it uses information, sharing vast amounts of data and joining up services and systems on an unprecedented scale. Use of the Internet is expanding; information can increasingly be accessed anywhere at any time.

In this rapidly changing environment, is the public sector's information adequately protected against deliberate attack, disruption to services or loss of critical data?

The Cabinet Office commissioned this independent review, well before recent losses, as part of the work to ensure government keeps pace with these changes, to assess how well government is protected now and in the future. The review was asked to report back on:

- whether Information Assurance across government is adequate enough to provide stakeholder confidence in the government's information infrastructure
- whether information and services are protected in a timely and cost-effective way
- the extent to which current investment in Information Assurance will support the requirements of shared services and the *Transformational Government* agenda.

Key recommendations from this work were published in a synopsis of this work in June 2007 in order to be able to inform the direction of the National Information Assurance Strategy delivery plan.

How well is government doing?

The review identified that, although measures are difficult to come by, most departments are now investing significant amounts of money and effort in information security. There are areas of good practice, but there are also many areas where government must improve.

- Government must do more to deliver confidence in its information infrastructure; enabling Information Assurance and enhancing Governance; Information Risk Management; Policy and Operations; and Monitoring and Control.
- Capabilities have developed in silos (within individual departments) which has resulted in complexity in joining up, and limited re-use across Government with many different areas of government addressing the same challenges differently.
- The challenge now is to enable joined up government, which means connecting to more environments and sharing more data in an environment that is increasingly more hostile.

Government departments are actively trying to address these challenges; however, at the time of my review, adequate mechanisms were not yet in place to support them in achieving this and these will need to be put in place, or the Government's aspirations for service delivery enabled by technology will be at risk.

The Data Handling Review has identified a set of actions for government which should deliver enhanced Information Assurance mechanisms and capability across government.

In essence Information Assurance is progressing within departments; but in a joined up world, where data and services need to be connected and layers of trust need to be established, new thinking and new mechanisms need to be put in place.

Strategic Recommendations

Government going forward needs to be able to demonstrate a comprehensive understanding of the risks it is facing. It needs to put in place clear policies that mitigate the risks; to monitor performance for compliance, and ensure that there is capacity to respond to incidents.

The current mechanisms and approaches need to be sharpened to assist government to deliver Information Assurance in the current and future planned operating environment. Government should focus on the ten elements necessary for successful Information Assurance (IA) listed in chapter 4 of this report.

Key Recommendations:

A summary of key recommendations are put forward. The detail behind these recommendations can be found in the main body of the report. It is recommended that Government:

1. Creates a vision for Information Assurance and that this vision is incorporated into existing vision statements; laying out for citizens and other stakeholders what it considers are acceptable parameters for the sharing, management, and protection of information held and managed by government.

2. Create a new approach for reviewing and managing information risks across government. Enable new mechanisms to enhance the effectiveness of information risk management including a central facility for sharing risk information.

3. Mandate *board owners* to report quarterly on information risks and performance backed up by an annual audit of department's capabilities. Within this, establish clear metrics for managing performance of suppliers.

4. Provide the Prime Minister with a summary of Information Assurance across government and associated spending required to deliver cross government security associated with Information Assurance.

5. Simplify the complexity of the twenty five plus working groups and structures in this area. Enable one central mechanism for developing coordinated joint working, for sharing best practice and for establishing information assurance priorities across departments and agencies.

6. Create clear mandatory *policy* rules on security across government. Define minimum standards that departments sign up to. Enable independent monitoring for compliance.

7. Tackle *identity management* challenges through mandating the use of privacy impact assessments. Specify standards of protection for identity registration, management and use in government and the wider public sector.

8. Mandate *professional certification* for those working in Information Assurance in every government department across key defined roles. Ensure citizens, employees and other stakeholders are educated on information assurance and what is expected of them.

9. Measure security through audit and monitoring to a defined standard. Mandate the reporting of incidents to an independent organisation responsible for capturing incidents and ensuring investigations are conducted to a given standard and lessons are learned.

10. Have an *independent oversight* capability retained by government who can be called upon to give independent oversight and advice on Information Assurance to give stakeholders confidence. Provide this capability in addition to the formal regulatory roles that exist outside government.

1. Introduction

1.1 Purpose of this report

Government is transforming the way it uses information, sharing vast amounts of data and joining up services and systems on an unprecedented scale. More and more information is increasingly held and shared relating to citizens and business, the business of government and national security. A change in the way government is working is bringing new opportunities – and new challenges. The question now is whether that information is adequately protected in government?

The Cabinet Office commissioned this independent review to assess how well government departments and agencies are meeting the challenges of Information Assurance. This report presents the findings from the review.

1.2 Scope of the review

The review covered government departments and agencies in the United Kingdom. It covered all aspects of Information Assurance including availability of information, integrity of information and confidentiality and privacy of information.

The focus was to make an independent assessment of Information Assurance capabilities in the UK government and its departments and agencies and to specifically report back on:

- whether information assurance across government is adequate enough to provide stakeholder confidence in the government's information infrastructure
- whether information and services are protected in a timely and cost effective way
- the extent to which Information Assurance will support the requirements of shared services and the *Transformational Government* agenda.

1.3 The changing context

Stakeholders expect government departments and agencies to have protection in place wherever information is held; they expect government to have adequate safeguards in place and they expect government to be making sure these safeguards are effective.

New initiatives such as Contact Point capturing information on children, the new Connecting for Health system, the National Identity Register, and enhanced national security systems are just some examples of the increased need for effective Information Assurance.

The risks are also changing significantly. The potential loss of information and the impact that can have on service delivery have become very visible. Other risks including fraud, espionage and potentially terrorism are also driving the need for adequate Information Assurance.

Given this context, the review was asked to focus on whether Information Assurance is adequate for stakeholders to have confidence and whether it is being provided in a cost effective manner.

1.4 Structure of the report

This report is presented in six chapters:

1. Introduction – purpose and context of the review (this chapter)
2. The changed environment: new challenges
3. The operational risks
4. What success looks like: principles for effective Information Assurance
5. Findings from the review: how well is government doing?
6. Recommendations

2. The changed environment: new challenges

This chapter outlines some of the main features of the changed environment and the new challenges associated with change.

2.1 Overview

Government is joining up and sharing data and services. Departments and agencies are changing and enabling new ways of delivering services to the citizen, all the way from benefit services through to national security.

2.2 Examples of change

Some examples of this transformation, and their dependence on Information Assurance, can be seen below

- In one week, the National Health Service sends 1.4 million prescriptions electronically. 437 million medical records have now been digitally captured, and over 400,000 users are now able to access patients' clinical records electronically.[1]
- Every month, the Police National Computer handles 10 million transactions. Police officers can now also use new technology to take and match fingerprints at the roadside on handheld devices.[2]
- The new Defence Information Infrastructure will reach 300,000 users on 150,000 terminals at almost 2,000 Ministry of Defence sites around the world.[3]

2.3 Main features of the changing environment

The main features of the changing environment are:

- The rapid pace of technological change
- Information sharing on an unprecedented scale
- A dependence on electronic information that is available and reliable, and secure
- A global delivery model – not directly controlled by government
- Expectations of a balance of privacy and security.

2.4 The pace of technological change is accelerating

Government spends 14 billion pounds per year on information technology and is bringing in new electronic services at a faster rate than ever before. There are now significant numbers of technology projects using increasing amounts of new and unfamiliar technologies in the public sector.

[1] NHS Connecting for Health statistics 26th November 2007.

[2] Transformational Government Annual Report 2007.

[3] Transformational Government Annual Report 2007.

2.5 Information sharing on an unprecedented scale

The growth of the transformation has also combined with a need to share data on an unprecedented scale with more and more users accessing information.

For example, the DVLA now shares data in a controlled way with more than 23 different countries and in the UK with over 400 local authorities, 42 police services and many private sector organisations.[4]

2.6 A global delivery model – no longer directly controlled by government

The majority of government departments and agencies now rely on third parties to handle most of their information and services. Services are often contracted out and increasingly outsourced and off shored.

The government now buys services from organisations located all around the world. Many assets are often no longer under British ownership and delivery capability can be outside the legal jurisdiction of the UK.

The different data protection laws outside the UK, the reliability of some overseas supply and the activities of foreign intelligence services are now presenting new challenges for the Government.

2.7 A dependence on information stored only in electronic format

Key services now depend on electronic information; physical data records are rapidly becoming obsolete. Much information is stored now in electronic only format.

Dependence on the availability of electronic-only information is unprecedented; and this means that power cuts or other system breakdowns have the potential to bring many services to a complete standstill.

2.8 Expectations of a balance of privacy and security

To deliver transformed services, most groups recognise information needs to be shared in new ways. However, citizens and other stakeholder groups expect to see appropriate safeguards are in place and working effectively in order to have confidence using those new systems.

2.9 A new model – with unprecedented demands for Information Assurance

Government is changing the way it delivers its services – sharing information to gain efficiencies and to make services better and more effective.

The new model for government delivery requires Information Assurance at unprecedented levels, to provide confidence to citizens and other stakeholders that information being used and managed by the Government is not being put at an increased risk as these electronic services are deployed.

[4] Driver and Vehicle Licensing Agency (DVLA) May 2007.

3. The operational risks

3.1 Overview

This chapter outlines some of the risks identified in the changed environment. There are the risks to implementation of programmes, many of which are well understood in departments – the vast scale of the projects' complexity, introduction of new technology and joining up with delivery partners to share information, services and systems.

There is also now a different class of risk: a hostile environment for operational services, where fraud and e-crime are on the agenda and increased threats of terrorism and espionage exist. Some recent examples have demonstrated this, as shown below.

3.2 Fraud

Identity fraud costs the UK economy over £1.7 billion per annum.[5]

There is increasingly a commercial value to government issued credentials such as driver's licences and passports.

There has also recently been evidence of criminals targeting government departments and their agencies. Criminals set up to defraud the state or in some cases employees working within government using information derived from their place of work.

3.3 Accidental damage/loss

Accidents and natural disasters can have a high impact. Losses such as the recent cases of HMRC and other organisations have highlighted the risks in relation to data.

Floods, and accidents such as the explosion of the oil refinery at Buncefield have also highlighted the challenges for the availability of services. A number of public sector organisations suffered data loss at a neighbouring site destroyed by the resulting fire. The Police National Computer had a key data centre at this facility which was totally lost. However on this occasion the service continued to operate normally from another facility and there was no outage to the service.

3.4 Espionage

The Security Service reports that a number of countries continue to devote considerable time and energy trying to steal our sensitive technology on civilian and military projects, and trying to obtain political and economic intelligence at our expense. They do not only use traditional methods to collect intelligence but increasingly deploy sophisticated technical attacks, using the internet to penetrate computer networks.[6]

[5] Home Office Identity Fraud Steering Committee (IFSC) February 2006.

[6] British Security Service, November 2007.

3.5 Cyber attack

In the UK numerous websites have recently been defaced including those of departments such as the Department for Environment, Food and Rural Affairs. In other countries there have also been incidents – in Estonia in 2007 government ministries and banks were overwhelmed by a series of cyber attacks.

> "The attacks are relatively low in sophistication, but have been highly effective due to the large number of compromised machines involved. Several of our constituents have expressed concern about how the UK government could defend against such attacks in the future. It is difficult to defend against a sophisticated Distributed Denial of Service attack without impacting legitimate business use. The best defence against these types of attack is to ensure that you have appropriate monitoring to detect the onset of an attack and a comprehensive business continuity plan in place that provides contingency against such attacks."
> *Source: British Security Service: Centre for the Protection of National Infrastructure*

Those working in government are increasingly aware that more sophisticated threats could emerge in the coming years. It is not inconceivable that in future years those wishing harm upon the UK could undertake similar electronic attacks.

3.6 Insider threats

Information leaks are one example of insider threat, arising from dishonest officials, or the placing of compromised people into organisations or using social engineering techniques in order to extract information, all of these are now being seen in the public sector.

3.7 A new environment where accidents, deliberate or targeted incidents cause substantial damage

Recent experiences here and abroad in the public and private sectors have demonstrated a new set of risks for government. Risks experienced are not all about national security. Information theft is now much easier and more profitable than conventional forms of organised crime and carries less risk for the criminals. New risks around data accuracy where information can be easily shared and interpreted incorrectly are also greater as connectivity and collaboration has increased.

There is also the global dimension associated with increased Internet use and the ability to attack and disrupt from a distance. New ways of working also pose additional risks, whether accessing information remotely, connecting new environments together, on the move or working in the home environment.

4. Principles for successful assurance

4.1 Overview

This chapter investigates what success might look like: the review identified four areas necessary for delivering successful Information Assurance.

- Leadership and Governance
- Information Risk Management
- Policy and Operations
- Monitoring and Compliance

4.2 Key Principles

The review identified key principles that need to be accepted for successful Information Assurance. Principles drawn from work done by other governments are:

- That public sector delivery requires information security and assurance.
- That information security practices need to reflect the changing environment.
- The government is a single entity; individual departments affect government as a whole.
- Professional skills for government are needed to support information security.
- Decision-making requires continuous risk management.

4.3 What should we be aspiring to?

In order to make these principles reality working within the four basic areas outlined above, government needs to achieve the following:

Leadership and Governance

1. Strategy, vision and direction
Have a clear vision of what will be looked after and in what way. Enable stakeholders to understand what information will be stored and shared for what purposes and what safeguards can be expected for that information.

2. Governance and accountability
Have clear lines of accountability. Ensure risks are owned, and that they are reviewed regularly. Make sure that where success is achieved, people are rewarded; where failure occurs, people are held accountable.

Information Risk Management

3. A proportionate risk managed approach
Have clear understanding of risks (the threats, the vulnerabilities and the likely impact) and what is an acceptable risk. Identify and manage risks and learn from the risk experiences of others. Assess risk continuously and be aware of upcoming risks.

Policy and Operations

4. Articulate requirements (policy)/minimum acceptable standards
Have clear policies. Make sure that policies are followed and kept up to date and that they are kept in line with business requirements and appropriate risk management decisions, and that policies are enforced and delivered throughout the organisation and its supply chain.

5. Structure, roles and responsibilities
Have clear roles and responsibilities. Ensure individuals and units are clear about their responsibilities across the organisation. Define clear structures for sharing experiences and enabling collaborative working.

6. Skills and expertise
Ensure that key personnel have the knowledge and experience to be able to build, design and deliver Information Assurance, both in government and its supply chain partners.

7. Assured enterprise architecture
Have access to technology that is affordable, secure and reliable. Have reusable solutions that are built on 'best of breed' and where others already have experience of their effective use.

8. Contracted delivery
Have security embedded into delivery contracts with suppliers. Have frameworks in place to enable clear effective measurement of those providing services to government. Have incentives and penalties in place to reward performance.

Monitoring and Compliance

9. Verification and testing
Verify that the appropriate level of security is in place and appropriate for 'go-live' when implementing new systems and services. Have assurance of whole systems rather than just testing of individual technology components.

10. Monitoring, auditing and breach reporting
Have a good understanding of what is going on in the operational environment. Have monitoring in place, have a place to report breaches, investigate properly and be ready to react in good time if things go wrong.

5. Findings from the review: how well is government doing?

5.1 Overview

This chapter presents the findings from the independent review. The review examined the principles and key success factors identified in the previous chapter, taking evidence and testing assumptions with various organisations, at multiple levels. The main findings are summarised below and then expanded on in the following parts of this chapter. The findings have been updated with an understanding of what the Cabinet Secretary's Data Handling Review will recommend. At this stage it is too early for this review to determine how well these are being implemented in departments. This should be done after an appropriate period of time.

- A **vision** for shared services, data sharing, national security and transformational government has been set, but remains to be translated into a vision for Information Assurance across government.

  The move to develop Information Charters across government should enable citizens and other stakeholders to understand how their data is being captured and used.

- **Accountabilities** around Information Assurance do exist at board level in departments and agencies; mechanisms for holding people to account and ensuring that responsibilities are being carried out need to be sharpened.

  The announced move to cover Information Assurance in the Statement of Internal Controls is welcomed and should improve the position in this area.

- **Risk** processes for managing overall business risk are in place; however, more attention needs to be spent on identifying and managing information risks. Performance varies across the public sector and appraisals can be subjective.

- Government wide **policy** around around Information Assurance is complex and should be clearer. The lack of simple, clear guidelines is causing policy to be variable across departments and reduces the overall effectiveness of Information Assurance.

  The review to clarify and simplify policy and standards is welcomed and should, if properly done, improve the current situation.

- The **structure, roles and responsibilities** of the committees have evolved over a number of years. There are currently some 25 plus working groups and committees making collaboration across government complex and expensive. The recently announced commitment to consolidate these groups is welcome.

- Government is driving forward **professionalism** in Information Assurance. There is a high variance in skills and experience. The framework for professionalism has been developed. However, this still needs to be embedded across government.

- The public sector is becoming a more 'intelligent client' in terms of **secure contracting**. Purchasing has improved greatly, but supplier management remains an issue and is an increasing challenge across government.

- **Testing** mechanisms are in place. However these do not always adequately test operational readiness. There are also not many products in the market that have been tested, and departments often deploy solutions before approvals are awarded. The process for testing needs to be enhanced.
- **Monitoring** and **Compliance** across government is variable. Departments whose approaches are well advanced now have to connect to areas where Information Assurance is less robust giving rise to challenges across government as a whole. The recently announced enhanced compliance mechanisms are welcomed and should address some of these issues.

5.2 Strategy, vision and direction

A vision for shared services, identity management, data sharing and transformational government has been set, but remains to be translated into a vision for Information Assurance across government.

Different environments have different visions in terms of what level of protection is necessary. These create a lack of clarity as to what safeguards citizens and other stakeholders can expect in the protection of their data.

5.2.1 Different department visions

For example, in the area of children's information, Contact Point will enable authorised practitioners across education, health, social care, youth justice and the voluntary sector to find out who else is working with a child or young person.

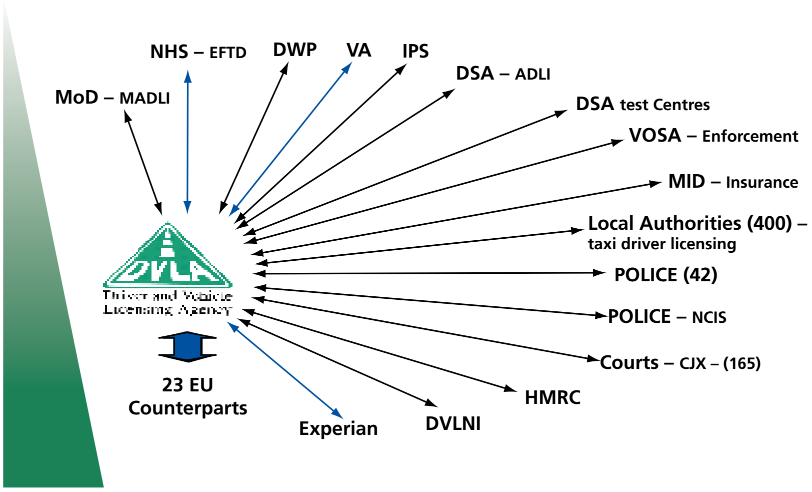
However the systems of the NHS and those of Contact Point were never originally designed to work together. The National Health Service are currently working with Department for Children Schools and Families to get the security architecture and related processes right for the NHS data sets- this is work underway but not yet completed.

The lack of a centrally defined and coordinated vision across government of what information needs to be protected at what level has created significant challenges, including for joining up services.

5.2.2 Different Country Visions

The Driving and Vehicle Licensing Agency (DVLA) understands the concepts of Information Assurance; however, they are facing additional challenges. The organisation is now receiving requests for information from across the EU, as well as from other government departments and the private sector within the UK.

Who does DVLA share Drivers data with now?



These requests have the potential to set precedents for the UK Government in handling and protecting information. However there is not a sufficiently worked through supporting vision available to DVLA setting out what is acceptable as a national framework.

The government data sharing vision states "We must, of course, properly use the provisions in the Data Protection Act as a safeguard to protect privacy and confidentiality but it must not be used to justify unnecessary barriers to sharing information".[7]

However data protection practices differ internationally and therefore adequate consideration needs to be given as to how to ensure that these standards are maintained in environments where different laws operate.

The impact

Citizens and other stakeholders do not know what they can expect from government in terms of protecting and safeguarding information. Some departments take higher risks than others; a shared vision is emerging, but until this is fully realized there will continue to be significant challenges in joining up.

5.3 Governance and accountability

Accountabilities around Information Assurance do exist at board level in departments and agencies; mechanisms for holding people to account, and ensuring that responsibilities are being carried out, need to be sharpened. The announced move to cover Information Assurance in the Statement of Internal Controls is welcomed and should improve the position in this area.

5.3.1 Accountabilities in Departments

Departments do now all have a responsible person at board level that is accountable for managing information risks in the department. However more needs to be done to ensure improved accountability for managing information risk in departments and agencies.

The Department for Work and Pensions is an example of a model that shows clear governance. Accountabilities are defined to board level, outlining who is responsible, who is accountable and who should be consulted and informed. (See table below).

What	SIRO	Business Unit CEO	Department CIO
Business Unit Risk Management	C	A	C
IS/IT Risk Management Assurance	A	R	R
IS/IT Risk Management Delivery	C	R	A

A = Accountable; R = Responsible; C = Communicated or Consulted

The Ministry of Defence has recently set up an Information Risk Management Group (IRMG) which will now enable an enhanced mechanism for managing information risks.

The challenge for these and other departments is to make sure that the model translates through to the operational environment. There are need to be robust identifiable mechanisms in place across government for users to show compliance, as there are currently too few at the operational layer.

[7] Government Vision for Data Sharing; September 2006.

5.3.2 Cross Government Accountabilities

Just over half of the departments in the review considered that risk owners for cross-government systems are clear; less than half were clear about how that translated into departmental responsibilities for cross-government systems.

The Government Secure Intranet (GSI) is one area which demonstrates the complexity of shared services. The Office of Government Commerce (OGC) is the Contract Manager for the GSI, the National Technical Authority (NTA/CESG) is Advisor for the codes of connection to connect to it, and the Cabinet Office (CSIA) is accountable for accreditation of the service itself.

There are many GSi Codes of connection. The GSi 'family' of networks has over 450,000 users, 200 customers with different codes of connection for each of the 5 key areas of the network.

The Cabinet Office (Shared Services) has an experienced Senior Responsible Owner in place who is accountable for the GSI, owning the business case and the aggregated risk. Holding people accountable in a system with so many users and stakeholders is complex and difficult.

5.3.3 Independent Oversight/Accountabilities

There is a regulatory role in the areas of data protection and freedom of information. There are also accreditors and internal auditors working within departments and agencies.

However no role exists to provide Independent Oversight that the appropriate Governance; Information Risk Management; Policy and Operations; and Monitoring and Controls around Information Assurance are in place across departments and agencies.

The Impact

Without clear accountabilities, visible metrics, and independent oversight in the design and running of Information Assurance within the Public Sector, trust in government may be undermined going forwards.

5.4 Proportionate risk management approach

Risk processes for managing overall business risk are in place; however, more attention needs to be spent on identifying and managing information risks. Performance varies across the public sector and many appraisals can be subjective.

5.4.1 Managing overall business risk

The processes for managing overall business risk in the public sector have been developed and adopted over a number of years now. Departments follow the Treasury guidance on risk (the Orange Book) and OGC guidance.

Identifying and protecting critical assets lies at the heart of the risk assessment processes in government. Yet there needs to be a more consistent way to look at this in the public sector for information risks. As well as a mechanism to relate this to the critical national infrastructure partners who the public sector is dependent on.

A new set of tools is being developed in the Centre for the Protection of National Infrastructure (CPNI) and these should enable organisations to identify critical assets and allocate resources accordingly.

In terms of understanding risks, every department works with risk registers but these vary in quality. Departments and agencies also use a variety of different sources for threat information and these sources also vary in quality and perspective.

5.4.3 Assessing risks

Departments tend to assess risks from their own perspective rather than considering the perspectives of others. Off shoring risks, for example, are assessed differently across government. Alternative approaches have emerged for addressing similar risks.

For off shoring generally, all central government departments have tended to take the CPNI advice into account, but then have separately developed frameworks for assessing risks; and no mechanism currently exists to share those frameworks.

In relation to personal data being held overseas, this has recently been reviewed by government and new measures have been put in place.

For assessing risks relating to personal information, Privacy Impact Assessments are used in other countries.[8] This is an assessment tool that describes the personal information flows in a project, and analyses the possible privacy impacts that those flows (and the project as a whole) may have on the privacy of individuals. These tools are not yet used as standard practice in the UK.

5.4.4 Addressing risks

Most departments report that information risk is included as an integral part of examining other organisational risks in key projects.

Risk calculations (often known as IS1[9] risk calculations) are supposedly used to manage information risk in a particular project or programme, however, they are very technically focused and can be overlooked in business risk discussions.

In addition accreditation documents capturing risks for a particular system do not always describe the information in a way that can easily be captured in the risk register.

The impact

Risk assessment is patchy leaving many without a clear understanding of the risks they are facing or exposing their stakeholders to. Enhanced risk processes would enable easier, faster and more cost effective joint working and improved confidence for stakeholders.

5.5 Policy/minimum standards

Government wide **policy** around around Information Assurance is complex and should be clearer. The lack of simple, clear guidelines is causing policy to be variable across departments and reduces the overall effectiveness of Information Assurance.

The review to clarify and simplify policy and standards is welcomed and should, if properly done, improve the current situation.

[8] Government of Australia, August 2006.

[9] Information Security Standard 1.

5.5.1 Central Government Policy

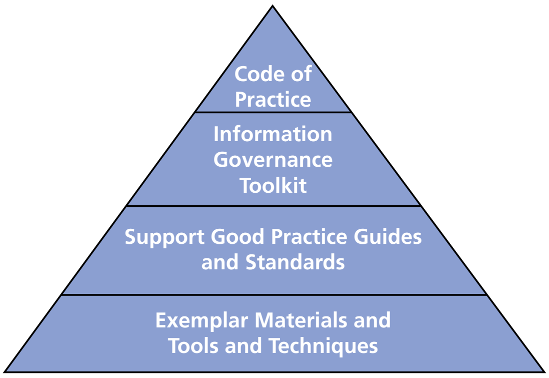
Government policy contained in the Manual of Protective Security (MPS) is currently being updated. At two thousand pages long, it was designed in a Cold War era and was last fundamentally reviewed in 1994. It focuses on physical security, Information Assurance and personnel issues, but does not yet adequately address the current and future challenges of Transformational Government, shared services and shared data.

There is however plenty of useful guidance in the MPS, but departments are encouraged to interpret their own view of policy in line with their own business requirements.

5.5.2 Different Departmental Policies

The MPS is also not the only policy in government. There has been a lot of focus on developing Information Assurance policy within departments The Ministry of Defence, for example, uses JSP440 which was originally structurally built upon the MPS but then adapted for the specific needs of the military.

The National Health Service has developed their own frameworks as they do not follow the MPS. The NHS framework can be seen below.


Code of Practice
Information Governance Toolkit
Support Good Practice Guides and Standards
Exemplar Materials and Tools and Techniques

The NHS Information Security Framework

Trying to join up different departments is complex. For example when the Health Service which uses the NHS Framework has to collaborate with the Department of Children, Schools and Families (which uses the MPS) or the Military (which uses JSP 440) there are immediate challenges and inconsistencies.

5.5.3 Different Codes of Connection

There has also been much good work dedicated to developing codes of connection to government services. The networks connecting these environments and others across government are governed by codes of connections.

There are many such codes of connection. The GSi family of networks has over 400,000 users, 200 connections and some 153 customers with different codes of connection for each area of the network. The N3 network has an estimated 1.2 million users in the Health Service and the Criminal Justice network CJX has 150,000 users.

Each code of connection is different and in some cases take different approaches. Exceptions are allowed with the consent of affected parties. These exceptions can cause further ambiguity about the exact level of security being applied.

Enforcement of policy varies. Codes of connection have to be signed with supporting evidence where appropriate, but these are seldom inspected in the operational environment.

Common standards would be more cost-effective and improve the confidence between transacting parties. Where policy is voluntary or it is unclear how it is actually deployed, it is difficult to understand what is in place and thus the extent to which information is protected. The impact can be particularly seen as government moves to shared services – as in the example below.

5.5.4 Common Standards

There are some government departments and agencies now working together to agree common standards. The Identity and Passport Service and the DVLA (Driver Vehicle Licence Agency), for example, have worked hard to agree common standards for photographs so that this type of information can be shared and re-used effectively.

Passport photographs are now stored and transmitted electronically to the DVLA so that they can be reused in the application process for a driving licence.

However across government generally there are currently multiple different ways of looking at identity management. There are also multiple access control mechanisms. Fewer mechanisms based on common standards would improve Information Assurance.

The impact

Departmental differences in policy make it more complex to collaborate, and more costly to maintain policy. Exceptions to central policy are often allowed making it difficult to have confidence in government Information Assurance, and some shared service environments are now not trusted by users, resulting in extra expenditure.

The implementation of the Data Handling Review should help address some of these issues with its focus on mandatory minimum standards.

5.6 Structure, roles and responsibilities

The structure, roles and responsibilities of the committees have evolved over a number of years. There are currently some 25 plus working groups and committees making collaboration across government complex and expensive.

5.6.1 Multiple different stakeholders/roles

In departments there are multiple roles participating in Information Assurance. This is one demonstration of how much effort departments are committing to the challenges of Information Assurance.

These roles include the Senior Information Risk Owner (SIRO), the Chief Information Officer (CIO), the Departmental Security Officer (DSO), the IT Security Officer (ITSO) and the Accreditor working for a Senior Responsible Owner (SRO).

Some areas have a full time Departmental Security Officer. Others combine this with other roles such as facilities manager. Despite the titles often being consistent the interpretation of the role is often different, which makes collaboration across government complex.

In addition, knowledge of the individual can be limited as some responsibilities at the senior level are transferred frequently. In the case of Board level responsibility for Information Assurance in twenty two departments (out of 28) this has changed at least once since 2004. One department has changed this responsibility three times in two years.[10]

[10] Cabinet Office Central Sponsor of Information Assurance 2007

5.6.2 Committees and Working Groups

There are some twenty five plus working groups and committees involved in Information Assurance across government, ranging from policy to technical operations. The respective responsibilities of the various groups can be confusing and should be clarified. The Data Handling Review makes a commitment to consolidating these groups and address these issues.

In addition the governance and reporting structures at the centre add to the complexity. The Cabinet Office, the Foreign Office and the Home Office all have cross government elements reporting into them, which can make cross government accountability for Information Assurance

New models are being developed. The CIO Council and CTO Council provide some good emerging examples of working together, with consistent group solutions being created to solve common problems.

One of the challenges is the need for Information Assurance to be driven by technology as well as national security. The current mechanisms e.g. the CIO Council and the Official Committee on Security are not yet fully integrated and it will be essential that this is achieved in order to deliver effective information assurance.

The Impact

Some committees and working groups offer valuable networking opportunities. The number of groups, the divergent reporting, and overlap of their effort is inefficient; these groups need to be more focussed on solving key challenges. More consistent roles and structures between departments would also make it easier to engage and collaborate across government.

5.7 Skills and expertise

Government is driving forward professionalism in Information Assurance. There is a high variance in skills and experience. The framework for professionalism has been developed. However, this still needs to be embedded across government.

Departments expressed concerns about the adequacy of their in-house staffing for Information Assurance; In 2007 less than half considered that their capabilities were adequate to meet current and future Information Assurance challenges.

5.7.1 Professional Skills and Competencies

The competencies for an accreditor, for example, are defined and there are mechanisms in place to assess competency within the Information Security Training Paths and Competencies Scheme (ITPC).

However, the scheme is not yet mandatory so it is difficult to assess the level of competency in every department across government. The review did highlight a high degree of variance in skills and experience across departments.

The impact

Skilled people are difficult to find and retain, in particular because of wage differences between the public and private sector. It is currently difficult to understand the right level of skills and competencies exist in government to deliver the necessary security and Information Assurance.

5.8 Enterprise Architecture

Government is starting to re-use best practice and mechanisms are emerging, but the joined up approach needs momentum, given the volume of products and services needed to develop and to assure the changes of transformational government.

5.8.1 Sharing Services that are tried and tested

The principle of re-using 'safe' solutions tried and tested elsewhere will help ease this situation. Some early progress has been achieved. The Department for Work and Pensions shares its Payroll Solution with the Cabinet Office; the Cabinet Office has created the Flex project, a base desktop platform for those departments who can use it to run their systems.

There are contractual and cultural constraints to achieving re-used solutions across government and solving these challenges will take time. Although the logic is easy to understand, implementing it is another matter.

5.8.2 Development of common solutions

The Information Assurance Technical Programme which aims to establish communities where Information Assurance tools can be provided for a group of customers with common requirements, has had over £20million of funding.

This was originally focussed at those organisations at the upper end of National Security and those associated with the Single Intelligence Account.

The model is somewhat embryonic at the moment however offers significant potential for the future for capabilities to be developed centrally for the common good of government as a whole. A model for funding common requirements going forward will have to be formed as the current structure has no firm footing.

5.9 Contracted delivery

Government is becoming a more 'intelligent client' in terms of secure contracting. Purchasing has improved greatly, but the real issue is that departments cannot be sure that what has been contracted is being delivered – until it is too late. Supplier management remains a key issue.

5.9.1 Contracting security through suppliers

Departments have put Information Assurance into their contracts and individual departments have concentrated to varying degrees on trying to ensure they have effective management reporting of security in their contracts. However, few have standard ways of measuring performance or penalties for non-delivery.

Less than a quarter of departments reported that they had a standard way of measuring the performance of suppliers who were critical to delivering Information Assurance; around one third of departments said that suppliers were providing accurate management information to give stakeholders confidence about Information Assurance.

The Impact

There is a risk that suppliers will accept financial penalties rather than deliver the level of assurance contractually specified. Government departments cannot always encourage suppliers to adhere to contracts thereby putting their operations at risk.

5.10 Verification and testing

Testing mechanisms are in place. However these do not always adequately test operational readiness. There are also not many products in the market that have been tested, and departments often deploy solutions before approvals are awarded.

Less than a quarter of the departments in the review considered that the products they required were developed and approved in time to meet their business need. A direction has been set out to enable Transformational Government but the capacity is not yet in place to deliver the assurance model.

5.10.1 New and Challenging Assurance requirements

The changes in government delivery models have created a huge volume of new assurance requirements and the current accreditation system cannot cope.

New types of suppliers are also requiring their products to be tested. Some of those putting technologies forward for testing do not have any previous experience of getting products tested. It takes time to get agreement to access the source code and real vulnerabilities can take time to fix.

This was seen in the case of Blackberry which took over a year for the government to get access to the source code and get the product ready for government use.

At the product level there is very thorough testing, however this does not address the operational deployment of the service. A new model is being conceived by CESG, National Technical Authority (NTA), engaging the private sector more to provide additional capacity in testing products and services.

The expansion of the capabilities of the NTA will help with the assurance requirements of transformational government. The expansion is welcomed but the governance of those relationships with the private sector remains a crucial area one which has yet to be fully defined.

The impact

Current testing models take time to deliver answers, causing departments in some cases to go ahead without complete understanding of the security of their systems. More re-use of proven solutions would reduce the risk of reputation and financial damage.

5.11 Monitoring, auditing and breach reporting

In common with the mechanisms to hold people to account, there is a need for a much stronger compliance regime, and tools to ensure compliance need to be enhanced, as currently the monitoring of systems and performance varies widely across government.

5.11.1 Internal Audit

More than half of the departments in the review reported that their internal audit function measures the application of standards such as ISO27001. However the reality is that not all systems are accredited to any standard across government. Government could enhance its approach developing more robust mechanisms based on industry standard mechanisms such as ISO standards for Information Security and Business Continuity.

Most compliance is by self certification and there is limited inspection by independent authorities to check on the self certifications.

5.11.2 Monitoring

In terms of active monitoring some departments are well advanced, but they increasingly have to connect to areas where the operating levels of Information Assurance are much less understood resulting in a lack of understanding of the real exposures these new connections bring.

Few organizations have visibility outside their environment and therefore do not easily understand the security of others areas with which they may be connecting.

5.11.3 Incident Reporting

Incidents are not reported centrally and it is difficult in many cases to ascertain that appropriate actions were taken and that lessons were learned across government departments and agencies.

With regard to personal data losses, new reporting mechanisms have been established, which should improve the position in this area.

5.11.4 Compliance

Compliance regimes vary across government departments. There are limited mechanisms for the users to confirm that they are in compliance or even aware of the security policies in operation in their environment.

5.11.5 Independent Oversight

Internal Audit and Accreditors provide reviews of systems internally within government departments and agencies. These are essential civil service roles which not only look at live systems but also those in development.

However, there is currently no independent oversight or formal role in place to give stakeholders independent assurance that the right level of Information Assurance is planned and operating.

The impact

Without compliance regimes, policy is less likely to be adhered to and individuals will assume their own risk judgements – sometimes doing things which are not in line with the risk that the organisation is prepared to take overall.

Unless there is monitoring across government it will be difficult to ascertain what the true level of security actually is.

In addition without an independent oversight capability it will be difficult to provide stakeholders assurance that adequate protection is being planned and operated in government.

6. Recommendations

6.1 Overview

This section outlines the key recommendations and priority areas that might be addressed.

6.2 *Key Recommendations:* a summary of key recommendations are put forward

1. The government creates a vision for Information Assurance and that this vision is incorporated into existing vision statements; laying out for citizens and other stakeholders what it considers are acceptable parameters for the sharing, management, and protection of information held and managed by government.

   The vision for Information Assurance is owned and agreed to by the whole of government and in doing so sets mandatory parameters for what can be shared, what cannot be shared; what needs to be protected and what does not. The vision covers the complexities of a shared services environment and the Global and European context and covers the availability and integrity of information as well privacy and data protection.

2. Create a new approach for reviewing and managing information risks across government. Enable new mechanisms to enhance the effectiveness of information risk management including a central facility for sharing risk information.

   Provide a central facility for sharing *risk information* and a central information risk register based on risks experienced by departments and their agencies. Have the centre invest in a core capability to understand the Information Assurance risks facing government. Ensure the level of information risk for critical assets is captured and addressed in departmental risk management processes.

3. Mandate *board owners* to report quarterly on information risks and performance backed up by an annual audit of department's capabilities. Within this, establish clear metrics for managing performance of suppliers.

   Require accountabilities be clearly set out in departments and programmes – as well as for shared services. Mandate board level owners in each department to report against standardised metrics. Have the Cabinet Office develop and issue these and within this, establish clear metrics for managing performance of suppliers.

4. Provide the Prime Minister with a summary of Information Assurance across government and associated spending required to deliver cross government security associated with Information Assurance.

   Identify within this submission the budget required to develop cross government capabilities such as the Information Assurance Technical Programme. Establish a clear governance model for cross government Information Assurance.

5. Simplify the complexity twenty five plus working groups and structures in this area. Enable one central mechanism for developing coordinated joint working, for sharing best practice and establishing Information Assurance priorities across departments and agencies

   Set as a priority the re-use of assets and the development of common requirements across government in the area of Information Assurance. Enable mechanisms to share experiences and create common solutions across parties with similar interests and challenges. Enable the sharing of metrics and scorecards of departments and agencies to assist in procuring solutions and the development of shared services.

6. Create clear mandatory *policy* rules on security across government. Define minimum standards that departments sign up to. Enable independent monitoring for compliance.

   Develop simple rules around Information Assurance. Have these rules defined for all aspects including people, processes and technology. Ensure policy is clear in regard to physical as well as electronic security and considers both national and international contexts. Make policy compliance a priority and ensure there are compliance tools available to departments and agencies. Include tools which can be deployed to check compliance at the user level. Ensure enforcement action is taken within three months where operations are identified to be non-compliant against policy.

7. Tackle *identity management* challenges through mandating the use of privacy impact assessments. Specify standards of protection for identity registration, management and use in government and the wider public sector.

   Re-use, where possible, tried and tested common standards around identity. Revisit the mechanisms around obtaining consent from stakeholders when data or information is used for purposes other than its original intention.

8. Mandate *professional certification* for those working in Information Assurance in every government department across key defined roles. Ensure citizens, employees and other stakeholders are educated on Information Assurance and what is expected of them.

   Define clear competencies and career paths for Information Assurance professionals. Establish mandatory professional certification for those working in Information Assurance in every government department and for contractors providing services to government. Provide appropriate remuneration for those achieving certification.

9. Measure security through audit and monitoring to a defined standard. Mandate the reporting of incidents to an independent organisation responsible for capturing incidents and ensuring investigations are conducted to a given standard and lessons are learned.

   Establish testing and monitoring in all departments to a consistent standard as specified by National Technical Authority. Establish a body for departments and agencies to report breaches and task that authority with the responsibility to ensure investigations are carried out appropriately and lessons are learned.

10. Have an independent oversight capability retained by government who can be called upon to give independent oversight and advice on Information Assurance to give stakeholders confidence. Provide this capability in addition to the formal regulatory roles that exist outside government.

Annex A. Glossary and Abbreviations

A glossary of terms provided by the Cabinet Office – derived from ISO 27001

Access Control	Control to ensure authorised access and to prevent unauthorised access to resources relevant to information security based on the business and security requirements.
Asset	Anything that has value to the organization.
Audit	Audit is the systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled.
Availability	The property of being accessible and usable upon demand by an authorized entity.
Business Continuity Management	A holistic management process that identifies potential threats to an organisation and the impact to business operations those threats, if realized, might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders reputation, brand and value creating activities.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Control	The means of managing risk, including policies, guidelines, practice or organisational structures, which can be of administrative, technical, management or legal in nature.
Impact	An adverse change to the level of business objectives achieved.
Information Security	The preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity and accountability.
Integrity	The property of safeguarding the accuracy and completeness of assets.
Organisation	A Group of people and facilities with an arrangement of responsibilities, authorities and relationships.
Privacy	The right of every individual that his/her private and family life, home correspondence are treated confidentially.
Risk	A Combination of the likelihood of an event and its consequence.
Risk Assessment	The overall process of risk analysis and risk evaluation.
Risk Management	Coordinated activities to direct and control an organisation with regard to risk.
Threat	A potential cause of an incident that may result in an adverse change to an asset, a group of assets or an organisation.
Vulnerability	A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Abbreviations

	Meaning
CIO	Chief Information Officer
CNI	Critical National Infrastructure
CTO	Chief Technical Officer
GSI	Government Secure intranet
HR	Human Resources
IA	Information Assurance
IATP	Information Assurance Technical Programme
CIPCOG	Civil Information Assurance Products Co-ordination Group
ICT	Information Communications Technology
IDM	Identity Management
NIAS	National IA Strategy
NED	Non-Executive Director
GIPSI	General IA products and services initiative
OGD	Other Government Department
PGA	Pan Government Accreditor
SIRO	Senior Information Risk Owner
TA	Threat Assessment
SIA	Single Intelligence Account

	Operating Units
CSIA	Cabinet Office, Central Sponsor for Information Assurance
CO-SPD	Cabinet Office Security Policy Department
CCS	Civil Contingencies Secretariat
CPNI	Centre for Protection of National Infrastructure
CESG	GCHQ National Technical Authority
ISS	Intelligence and Security Secretariat
OGC	Office of Government Commerce

	Regulation
HRA	Human Rights Act
FOI	Freedom of Information Act
DPA	Data Protection Act
RIPA	Regulation of Investigatory Powers Act
PCEA	Police and Criminal Evidence Act
CMU	Computer Misuse Act
OSA	Official Secrets Act

Annex B. Working Groups

Below are some examples of the working groups and committees involved in Information Assurance across government. The complexity of the reporting lines and work effort has been referenced in the main body of this report. Five groups have been removed from this list for reasons of national security.

	Groups and Structures
AAP	Airwave Accreditation Panel
AF	Accreditors Forum
CDF	Crypto Developers Forum
CIO Council	Chief Information Officer Council
CIPCOG	Civil Infosec Assurance Products Co-ordination Group
CTO Council	Chief Technology Officer Council
DIPCOG	Defence Infosec Products Co-ordination Group
ECRRG	Electronic Communications Resilience & Response Group
IACG	Information Assurance Collaboration Group
IAPPB	Information Assurance Policy & Programme Board
IARIG	Information Assurance Research Investment Group
IATP	Information Assurance Technology Programme
ISS	Identity Steering Group
ITSOF	IT Security Officers Forum
NGRMPB	Next Generation Network Risk Management Programme Board
NIAF	National Information Assurance Forum
MSPIE	Managed Service Provider Information Exchange
SARC	Security Accreditation Review Committee
SIRO	Senior Information Risk Owners Forum
TISAC	Telecommunications Industry Security Advisory Council

For more information about the CSIA go to www.cabinetoffice.gov.uk/csia

If you would like to comment on this, please contact:
CSIA
2nd Floor
26 Whitehall
London SW1A 2WH

Or email us at csia@cabinet-office.x.gsi.gov.uk
or direct to nick.coleman@cabinet–officed.x.gsi.gov.uk

© Crown copyright 2008

The text in this document may be reproduced free of charge in any format or media without requiring specific permission. This is subject to the material not being used in a derogatory manner or in a misleading context. The source of the material must be acknowledged as Crown copyright and the title of the document must be included when being reproduced as part of another publication or service.

The material used in this publication is constituted from 75% post-consumer waste and 25% virgin fibre.