

BCS, The Chartered Institute for IT
Consultation Response to
The Public Administration Select Committee's consultation on:
Good Governance – the effective use of IT

Dated: 21 January 2011

This page is left deliberately blank.

BCS, The Chartered Institute for IT

The Institute promotes wider social and economic progress through the advancement of information technology science and practice. We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

As the professional membership and accreditation body for IT, we serve over 70,000 members including practitioners, businesses, academics and students, in the UK and internationally. We deliver a range of professional development tools for practitioners and employees.

A leading IT qualification body, we offer a range of widely recognised professional and end-user qualifications.

www.bcs.org

PASC's consultation on Good Governance – the effective use of IT

Closing date: noon 21 January 2011

Consultation details: <http://www.parliament.uk/business/committees/committees-a-z/commons-select/public-administration-select-committee/news/iq-it/>

Summary of main points:

- 1.** Government technology policy can only be effectively implemented and the benefit realised through collaboration with the private sector and academia. Key success factors include the definition of core standards which will underpin sharing and re-use of information and all aspects of IT and information management.
- 2.** A centralised fiscal and managerial authority over cross-cutting programmes, together with centralised technical leadership are the principle keys to effective governance arrangements. The governance and management of all projects need to be raised to the level of the best, with the SRO role being embedded more comprehensively and universally in government managerial practice.
- 3.** To adapt to the environment of austerity, implementing new IT (eg to redesign existing systems) is necessary and will require investment. For IT implementation to be effective, it must be owned by the organisational executive and be seen as a business change programme supported by technology.
- 4.** In a 'post-bureaucratic age', IT's role is one that underpins and enables efficient delivery of public services.
- 5.** We welcome the important developments in the public sector towards professionalising IT such as the widespread adoption of SFIA in defining skills and roles. With the reduced use of external IT specialists and in some cases it has been drastic, we recommend that departments strive to retain an in-house core of IT specialists and a managed approach to outsourcing, to avoid projects failing due to diminished IT awareness and capability.
- 6.** The Government needs to maintain an awareness of new technological developments and contemporary business practices and skills to ensure a more effective exploitation of its investment in IT.
- 7.** We acknowledge that the Government's approach to information security and information assurance has improved significantly over the last decade and policy is more pragmatic and generally understood by users. However, we recommend that the Government adopt a more proactive and holistic approach in all areas of information security; in particular, in the area of privacy where appropriate governance should have a sense of a formal, clear and joined-up strategy.

Consultation Questions:

1. How well is technology policy co-ordinated across Government?

- 1.1 The UK Government published 'Transformational Government - Enabled by Technology' in November 2005 as the foundation for the implementation of change across the public sector. In January 2010 the Cabinet Office launched the 'The Government ICT Strategy', the strategy claims to be smarter, cheaper and greener founded on open source, open standards and re-use, for delivering the strategy for a more co-ordinated approach to IT policy. This strategy can only be effectively implemented and the benefit realised through collaboration with the private sector and academia.
- 1.2 The Institute would welcome the opportunity to contribute to this work before policies and implementation are finally agreed. Key success factors include the definition of core standards which will underpin sharing and re-use of information and all aspects of IT and information management. The Institute has significant expertise and intellectual resources to contribute to the agreement of standards. The appropriate use of open standards should be an integral element of the standards and policies. Given the wide range of activities across the public sector, care must be taken not to over-centralise while avoiding "reinvention of the wheel" which has undoubtedly taken place many times across government in the past.

2. How effective are its governance arrangements?

- 2.1 Accountability resides primarily at the departmental level in government, and we recognise that IT governance in major departments is generally well established. However, for activities which span sectors or other groupings of departments, the position is less well developed and with a few notable exceptions has not generally been effective. The lack of centralised fiscal and managerial authority over cross cutting programmes, together with absence of centralised technical leadership is the principle impediments to success.

3. Have past lessons from NAO and OGC (Office of Government Commerce) reviews about unsuccessful IT programmes been learnt and applied?

- 3.1 Senior level engagement in IT-enabled projects has improved significantly in recent years, with the importance of the SRO (Senior Risk Owner) role being recognised and implemented to various degrees. The Institute believes this trend needs to be embedded more comprehensively and universally in government managerial practice. The recent NAO report on projects recognised various improvements in the delivery of projects but again we believe that the governance and management of all projects needs to be raised to the level of the best, which is a prodigious task.
- 3.2 Analysis has consistently demonstrated that IT-enabled project failures are frequently caused by over-ambitious and unnecessary centralization and excessive adherence to detailed and unique specifications. In addition the need to adhere to historical contract specifications, eg LSP (local service provider) contracts, impedes competition where product improvement is driven by specification rather than market innovation.

4. How well is IT used in the design, delivery and improvement of public services?

4.1 There are examples in public service where IT is used well, these include the HMRC and the DVLA online services which deliver excellent citizen-focus online services. The National Programme for IT and Directgov.uk have replaced a previously chaotic system of delivery into a robust infrastructure which provides world leadership in the development of standards.

4.2 However, in the present regime of cost-cutting throughout the public sector the Government will be forced to adopt different ways for the use and application of systems at the local level, which will involve focusing on the redesign of information technology implementation, making the most of what is already in place. This may entail internal investment to realise benefits from existing systems. Government leadership needs to step away from the outdated idea that IT is expensive and difficult and recognise that efficient and improved delivery of public services cannot happen without investment. It is a recognised feature of IT implementation in all industries that the computerising of outdated procedures is likely to make them more expensive rather than less. Implementing new IT must be owned by the organisational executive and be seen as a business change programme supported by technology.

5. What role should IT play in a ‘post-bureaucratic age’?

5.1 IT is central to the effective delivery of modern administration. In a ‘post-bureaucratic age’, we should not lose sight of the business objectives and not become obsessed by the technical detail of the process. This key question must be at the centre of all future IT-enabled change to achieve the business benefit required.

6. What skills does Government have and what are those it must develop in order to acquire IT capability?

6.1 The Institute acknowledges the work done by the government IT Profession Board in driving important developments including the widespread adoption of SFIA for the definition of skills both for roles and individuals; the establishment of a Technology in Business fast stream for IT professionals; and a recent recommendation that all departments should define a set of senior IT roles for which appropriate qualifications should be mandated. Some departments have gone further in encouraging all IT professionals to obtain qualifications and memberships appropriate to their specialism and level. We believe this represents a good start on the way towards professionalising IT in government, and we would welcome the opportunity to work closer with government in the further development of IT skills, development and professionalism.

6.2 However, departments generally do not have the overall IT skills capability or capacity to meet their sometimes ambitious portfolios of change, and have often become over-dependent on the external marketplace. This situation has been exacerbated by the high degree of outsourcing of IT services, which makes it more difficult to develop and maintain the required level of client-side IT skills. Recent cost-cutting exercises have reduced, in some cases drastically, the use of external IT specialists but this has happened so quickly that there is a real risk of projects failing due to lack of IT capability. We believe that a more managed and balanced approach to the use of the external marketplace is required while departments work hard to increase their in-house capability.

7. How well do current procurement policies and practices work?

7.1 Current government procurement is clumsy, inefficient and plays to the very large systems integrators. Factors contributing to the inefficiency are as follows:

7.2 Excessive detail in specification and compliance management. Government should procure on the basis of the business benefit required and let suppliers propose innovative solutions which are likely to be more cost effective. This will require a different attitude and skill set in HMG procurement and a different approach to OJEU (Official Journal of the European Union: <http://www.ojec.com/>) interpretation and compliance.

7.2 Policies and practices across the public sector are frequently not written in plain language and vary fundamentally in approaches, leading to a poor understanding of requirements. Often outdated, complicated procurement policies and practices have led to the difficulties in procuring software, a main factor in causing IT projects to fail due to late deliveries and over budgeting. The difficulty in procuring software to government requirements in turn stifles competition and innovation.

7.4 The current lack of a best practice model to control delivery of software to time and budget means that keeping track of the unit costs of bought-in software, and the judging of value for money, will not have been embedded at a similar pace into the working culture of government departments.

7.5 To enable procurement policies and practices to work well, we recommend incorporating the following, in line with COSMIC's recommendations¹:

- Measurements of the amount of software required and delivered so that unit costs can be measured.
- A common repository of unit costs and other performance data from all public sector software-intensive IT projects which can be used to share experience and to support contract negotiations with IT suppliers.
- Processes by which customers can exploit the data to control and improve value for money and the delivery of new systems to time and budget.

8. What infrastructure, data or other assets does government need to own, or to control directly, in order to make effective use of IT?

8.1 The Government must own and control data and make certain that it is safely held and used responsibly. It must similarly ensure that the applications processing the data are trustworthy. Apart from the ownership and control of data, the Government do not need to own any assets or infrastructure.

9. How will public sector IT adapt to the new 'age of austerity'?

9.1 Proper management of public sector IT will be cost effective together with the recommendations mentioned in 4.2.

¹ Quote from Charles Symons, COSMIC, response submitted dated 11 Jan 2011.
Consultation response to PASC's Good Governance – the effective use of IT v5

10. How well does Government take advantage of new technological developments and external expertise?

10.1 In some cases very well as mentioned in 4.1 where developments are well designed and follow industry best practice and de facto standards.

10.2 There have also been cases where the Government had not taken advantage of external expertise. For example, no action was seen to be taken on southernSCOPE², a project management method for procuring software, proven to cut the average budget over-run to less than 10% and provide software value-for-money within the top 25% of industry best practice (extracted from COSMIC findings).

11. How appropriate is the Government's existing approach to information security, information assurance and privacy?

11.1 The Government's approach to information security and information assurance has improved significantly over the last ten years. Policy is more pragmatic and generally understood by users. However, the one failing is that policy is not mandated and this has resulted in serious breaches in recent times as seen in the case of the HMRC data loss. Senior Risk Owners (SROs) have been appointed in government departments thus ensuring that the subjects have full visibility at senior level. It is understood that a minister from each government department is being nominated as the owner of Cyber Security. Cyber Security brings new challenges as the threats are wide ranging, complex and not generally understood. In the Cyber domain, mandating policy is deemed essential. Policy documents issued by CESG are well written and easily understood

11.2 In some cases, the approach has been excessive in particular with network security making applications inaccessible and difficult to use. The key is to secure data at the storage and application level and use encryption to cope with the fact that networks are inherently insecure thus making accessibility much easier.

11.3 Knee-jerk reactions are reducing the benefits of IT systems. The current culture of 'report near-misses' in the public sector does not encourage openness and proactive action. A holistic, proactive and joined-up approach is to be encouraged to better prepare for the devolvement of services at local levels.

11.4 Following the high-profile data losses in recent years, we acknowledge that the Government has generally taken seriously its responsibilities to treat personal and other sensitive data with care, but there is a risk that as focus is moved to other issues the risks of data losses will rise again. The government's transparency agenda needs to be pursued with an eye always on the need to maintain personal privacy and protect sensitive data.

11.5 Privacy has not, in the Institute's opinion, been a sufficiently high priority for government in recent years. The surge in data sharing, which would in most cases be more accurately described as 'data disclosure,' has blurred the boundaries between data silos without a sense of proper governance or accountability for use. In particular, the collection, aggregation and retasking of data sets to respond to headline needs, without a sense of a formal strategy for data governance, has

² <http://www.egov.vic.gov.au/victorian-government-resources/e-government-strategies-victoria/southernscope/southernscope-avoiding-software-budget-blowouts.html>
Consultation response to PASC's Good Governance – the effective use of IT v5

eroded trust in the ability of public authorities to protect or properly manage personal information. Examples of such approaches include the National Identity Service, which brought together existing government databases for uncertain new purposes, or ContactPoint, which was driven by an intrusive new register without clear objectives.

11.6 Furthermore, the Data Protection Act (1998) provides insufficient guidance to stop these undesirable uses of data, and does not sufficiently empower individuals to take guardianship of their own information. Central government departments have been perceived as treating the Act as an obstacle to be overcome or circumvented wherever possible, and even if the Act is taken seriously, it appears to be treated as the maximum level of protection required, rather than as a minimum baseline for respect for the individual's data. This problem is exacerbated by the lack of powers provided to the Information Commissioner until just recently, and his office's apparent reluctance to use those powers against public authorities even where significant breaches have occurred.

11.7 These problems are not unique to the public sector, and there have of course been numerous high-profile privacy incidents arising from private processing of personal information, for example Facebook, Google, Phorm. However, in the private sector there is a greater sense of accountability for proper information governance, driven by competitive market forces: where a company fails to respect its customers' data, those customers have the ability to opt out or to take their custom elsewhere. That accountability does not exist for the majority of public services, and hence there is a need for stronger regulation within the public sector.

11.8 The Institute would welcome a broader and deeper adoption of the 'Privacy by Design' principles espoused by the Information Commissioner's Office: in other words, building proper respect for privacy (as opposed to a simple compliance with the Data Protection Act) into every aspect of information processing. This might most effectively be achieved by specifying minimum privacy design criteria for all systems that handle personal information (as opposed to those with a protective marking) and then making those criteria a mandatory part of the formal business case, OGC gateway review process, and accreditation process. Furthermore, accountability for failure to comply or thereafter to protect personal information should be more closely bound to the individuals responsible for system implementation and operation, rather than the public authority itself: the current approach of fining authorities for breaches of the Data Protection Act serves only to penalise service users rather than those responsible for proper governance.

12. How well does the UK compare to other countries with regard to government procurement and application of IT systems?

12.1 With regard to procurement and following the take-up of the recommendations mentioned in 7.5, Finland's Ministry of Justice has successfully completed a pilot resulting in achieving a unit cost of software of €300, down from a range of €500 to €1000.

12.2 The Chinese, Japanese and South Koreans have established repositories of software project performance data, managed by national research institutes, to which public sector bodies contribute data.

End
