



Transformational Government in a responsible way

IAAC Response to the Cabinet Office consultation paper on Transformational Government – Enabled by Technology.

IAAC welcomes the forward-looking strategy presented in the document “Transformational Government: Enabled by Technology” (“the Strategy”), expressing as it does the UK Government’s ambition to keep up with the hopes and aspirations of citizens and business in being both efficient and trustworthy.

IAAC believes that the achievement of a well-formulated ambition will affect society at large; both directly in terms of a more efficient government, and indirectly in terms of government leading the way for citizens and business to use and develop electronic services themselves. A clearer indication in the Strategy as to the practical steps required to achieve the stated ambition would be welcome.

Much can be said in support and/or improvement of the proposed strategy. From its position as a non-partisan, vendor-independent platform that aims *to advance Information Assurance (IA) to ensure that the UK’s Information Society can count on a robust, resilient and secure foundation*, IAAC will focus on those points of direct relevance to Information Assurance and, directly related to that, the issues related to the concept of identity, which is central in delivery of (electronic) services.

General underpinning principles

- The need for accurate and timely information about “citizens, businesses, animals and assets” is well recognized. The role of Information Assurance in enabling safe access and responsible sharing of data related to identity (of persons –legal and natural-, animals, assets) is also well recognised. This assurance needs to be explicit, thus ensuring appropriate trust at all levels.
- In order to benefit from new IT services, all types of user should want to use them. Services should be regarded by users as useful, pragmatic and affordable. This requires involvement of users in the design and development phase of new services. When done well, this will result in better, user-oriented services and buy-in from the outset.
- Last but not least, the detailed text in the Strategy could give the impression that it is all about implementing IT for delivery of government services. At all stages of the process it is crucial to keep the focus on what the Prime Minister so clearly states in his introduction; it is about government living up to the hopes and aspirations of its users in being efficient and trustworthy.

Specific issues

Information Assurance is key for achieving the ambition set out in the Strategy. From a security perspective, it is well understood that in the case of many public sector procurements seeking to deliver value for money, security is too often added on at the last stage or compromised in a bid to bring the project in under budget and on time. This is certainly true of projects within the private sector. IAAC feels it is important to take



account of Information Assurance at all stages of the delivery process, and is therefore concerned that security and Information Assurance issues are not explicitly articulated in the Timetable for Change (par. 52-56).

Many of the Information Assurance initiatives mentioned in this paper are already underway. Nonetheless, it is important to convey how such initiatives will evolve to *meet the needs of the changing environment*. For example, if the expansion of service delivery channels is to be pursued, the security requirements will change. The Strategy places a great focus on the use of mobile devices as a means to interact with government. We feel it is therefore important that assurance considerations are made, explicitly, regarding such devices. Furthermore, IAAC notes the publication of the Information Assurance Governance Framework by the Central Sponsor for Information Assurance and would recommend that this document be referenced in any communication about the Strategy.

Proper **Identity Management** has two prerequisites: <1> data need to be attributed to identities in order to be useful for actions and transactions; <2> the identity of actors with whom information is shared or transactions are pursued needs to be beyond doubt. Without proper identity management the transformation cannot take place.

In the Strategy government expresses its ambition of developing a holistic approach to identity management, which should enable provision of trusted services (par.39/7). It also announces a new Ministerial focus on finding and communicating a balance between privacy and efficiency with respect to data sharing (par. 39/4). In order to support developing insight into this, IAAC is rolling out a consultation process in which government and industry stakeholders will meet with academia and international experts. It is IAAC's intention to deliver an Identity Assurance Roadmap for the UK by July 2006, which will aim to provide a base line insight and inform government and industry policy making.

Detailed comments

- ❑ The introduction of a requirement for all new public sector IT to have shared services mandate (par. 40) in order to pass the "value for money test" may complicate the process of procurement of public sector IT even further. This challenge needs to be addressed, explicitly.
- ❑ It may be useful to consider the specific impact of new models of Internet usage – e.g. web services, federated identity – and the possible disruptive effects of new and emerging technologies.
- ❑ Par. 37 – 'promotion of responsible channel choice'. Customer Group Directors will have to find the right way to inform citizens how much more efficient using electronic channels is, in order to prevent disenfranchisement of the digital 'have-nots' or 'don't-wants'. A 'user-centric approach' would suggest involving users in designing and developing such service delivery platforms.
- ❑ Par. 39.6 - 'The Government will further develop its risk management model'. In developing this model it is important to take explicitly into account the risks resulting from joining up previously stovepiped systems. Furthermore it should be noted that the transfer of risk between departments is not well handled, today, (e.g. as shown by the Bichard Report). This is a general governance issue that should be addressed, explicitly.