

Directors' Roundtable for Information Governance Wednesday 24 November

Purpose

This paper offers the Roundtable opportunities:

- A. to use IAAC's comments about information governance as one basis for further discussion at the Roundtable;
- B. to discuss IAAC's position on the particular issue of a governance regime for a National Identity Infrastructure (NIdI), responsible for all citizens' personal identity information.

Context

In 2002 IAAC was the first UK research organisation to examine the Information Assurance issues associated with corporate governance. The executive summary of the 2003 IAAC paper "Corporate Governance and Information Assurance" is attached at Annex A.

More recently, IAAC undertook a research programme from 2006 to 2008 on the subject of identity assurance (IdA). A key recommendation of the final report¹ involves NIdI² governance; other recommendations deal with requirements and operation of the infrastructure.

IAAC IdA recommendations

IAAC's report strongly recommends that the UK Government develops an Identity Governance Action Plan and, within that, should work swiftly to develop, agree and deploy an Identity Governance Framework for the UK.

The report also recommends that the UK Government should ensure that proposed governance arrangements are widely debated and agreed; UK should move quickly to put the governance arrangements in place as soon as possible, not just "in due course" as was indicated in "Transformational Government".

¹ The IAAC IdA report was summarised for the IAAC Annual Symposium in September and will be formally launched later in the autumn.

² A National Identity Infrastructure is likely to be an integrated mesh of public and private sector large-scale identity management systems (IMS) bound together by a number of central bodies, structures and processes, collectively serving and supporting a wide variety of personal, commercial and governmental identity-based needs.

Argumentation

The conclusions and recommendations reached in IAAC's IdA programme were based on the following points and issues:

UK's NIdI stakeholders do not have the same interests, aims or objectives for a NIdI. Robust arrangements are needed to resolve conflicts of interests.

NIdI governance is particularly important in order to safeguard citizen interests of their personal identity information.

Governance arrangements are needed from the outset of the creation of NIdI to provide the foundation on which the operations can be managed; governance cannot be retro-fitted. e

Proportionality is a key principle which will need to be defined carefully and comprehensively within the governance framework..

It is essential that data usage governance provisions be drawn up as fully as possible. Reliance on slowly evolving case law in lieu of proper governance from the beginning would allow questionable practices to be performed without due safeguards, thereby putting UK citizens' interests at risk.

The design and operation of the NIdI must not preclude identity recoverability. Importantly, the operation of the NIdI must not cause or permit the citizen's ability to authenticate themselves from outside the NIdI to wither.

It is inevitable that faults will emerge in the design or operation of parts of the infrastructure. For significant faults, the UK Government may need to suspend operation of the affected part of the NIdI until those faults are rectified or a suit-able work-around has been developed.

UK Government should limit the scope of the first generation of NIdI specifically to avoid the NIdI causing significant harms. Only once the UK has gained experience using an NIdI and has learned how the system fails can a more comprehensive NIdI be developed safely.

Annex A

CORPORATE GOVERNANCE AND INFORMATION ASSURANCE EXECUTIVE SUMMARY OF IAAC 2003 REPORT

The United Kingdom has an ambitious vision to build a Knowledge Society and to exploit the benefits of Information & Communication Technologies. However, this vision will only become reality if growing concerns over the lack of security in information networks are tackled. Trust and confidence are as vital to e-Commerce as they are to e-Government. Unfortunately, board-level awareness of these risks is not yet being translated into effective Information Assurance policies.

Responsibility for management of information risk rests with company boards. Directors of UK companies are increasingly aware of the importance of Information Assurance but they are not putting in place effective controls to manage the risks.

The market and soft regulation should be effective in ensuring that company boards manage information risks responsibly via the medium of corporate governance. Good corporate governance is critical to the successful running of a business. The Turnbull framework provides the foundation for a risk-based approach to corporate governance. However, increasing dependence upon ever more complex information systems means that more emphasis needs to be given to the information risk management element of corporate governance.

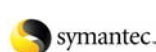
Information Assurance is a central component of business success and of a modern corporate governance framework. Assurance of a company's information assets is critical to realisation of stakeholder value and of business potential in an economy that increasingly relies on information technology and business transactions using the Internet. However, there is still a tendency to under value the importance of IA and to ignore the benefits that can be gained from improved security and providing more information and reassurance for users.

The involvement of senior management and the Board is a crucial factor in the success of IA strategies. Company boards need to understand the business benefits of Information Assurance; "scare stories" alone will not lead to genuine embedding of information risk management. Corporate governance guidelines, company law and sectoral regulations should be used to raise awareness amongst boards and stakeholders. Ultimately, market pressures to conform to "normal practice" are likely to be the most effective route to ensuring widespread take-up of IA policies as a way of managing information risk.

Board level awareness requires a clear business case, backed up by simple measures of effectiveness. Positive incentives include: marketing differentiation, increased shareholder value, reduced insurance premiums and an enhanced image for Corporate Social Responsibility. Negative incentives include: damage to reputation; legal liability; reduced shareholder value.

IAAC Sponsors

Registered Number 04326237



Once awareness is achieved, Boards need to implement effective controls. The starting point is implementation of a management standard such as ISO17799. This needs to be regarded as a minimum with which responsible organisations should comply, even if they are not certified.

Compliance with a management standard is only a start. In order to make effective decisions about risk in today's environment, Boards need to have more sophisticated tools at their disposal - in particular ways of measuring the benefits of particular solutions so that they can gauge how much assurance they are buying. Management standards need to be complemented by audit regimes; by the generation and sharing of risk data and by increased attention to dependency risks. In addition, the insurance market needs to be stimulated by information sharing and data acquisition.