RAND

Engaging the Board
Corporate Governance and Information Assurance

Andrew Rathmell, Stephanie Daman, Kevin O'Brien and Aarti Anhal

Prepared for The Information Assurance Advisory Council (IAAC)

RAND Europe

The research described in this report was prepared for the Information Assurance Advisory Council (IAAC). Further information can be found at www.iaac.org.uk.

ISBN: 0-8330-3508-8

Published 2004 by the RAND Corporation
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
201 North Craig Street, Suite 202, Pittsburgh, PA 15213-1516
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

For more information about RAND Europe or this document, please contact:
Newtonweg 1, 2333 CP Leiden, The Netherlands
Tel: + 31-71 524 5151
Tel: + 31-71 524 5191
www.randeurope.org
reinfo@rand.org

EXECUTIVE SUMMARY

- 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.

- 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.