

Compliance and Risk Management Risk Assessment and Mediation

Mark Serfözö
Chief Counsel, Compliance & Regulation
BAE Systems plc
PWC Eighth Annual Corporate Accountability Conference,
1 December 2009

BAE Systems plc, © Copyright 2009

“...profits are, in part, a reward for successful risk-taking in business...”

Turnbull Report, FRC October 2005

BAE Systems plc, © Copyright 2009

Contents

- The Woolf Report – a Road Map to Compliance and Risk Management.
- Identifying and Managing Non-Financial & Compliance Risks.
- The Role of Corporate Counsel – the Value Add.
- Remediation of Non-Financial and Compliance Risks.

BAE Systems plc, © Copyright 2009

The Woolf Report – A Road Map to Compliance & Risk Management

- The Woolf Committee was commissioned by the Board of BAE Systems in 2007 to provide a Road Map for the Company to become a global leader in ethical business conduct.
- The Woolf Committee was led by Lord Woolf and operated Independently. The Board undertook to implement the findings of the Committee at the outset.
- Report published in May 2008 and was a snapshot of how the Woolf Committee found the Company and provided recommendations for its ethical conduct going forward.

- The report is about:

“Business Ethics, Global Companies and the Defence Industry
Ethical Business Conduct in BAE Systems – the way forward.”



BAE Systems plc, © Copyright 2009

The Woolf Report – A Road Map to Compliance & Risk Management

- The report sets out the minimum level to which Global companies should aspire in terms of ethical business conduct, compliance and governance.
- The report made 23 recommendations to the Board of BAE Systems on actions it should take to achieve leadership in ethical business conduct among global companies. The recommendations fall broadly into 6 categories:
 - Governance, Board & Management
 - Leadership in Business Ethics
 - Code of Conduct
 - External Engagement
 - Future Contracting
 - Anti-Corruption & Compliance

BAE Systems plc, © Copyright 2009

The Woolf Report – A Road Map to Compliance & Risk Management

“...effective management of reputational risk by adopting high standards of ethical conduct should be at the centre of corporate governance in a global company.”

(Woolf Report 2008 –paragraph 4.28)

BAE Systems plc, © Copyright 2009

Identifying and Managing Non-Financial Risks

- A Non-Financial Risk is not a risk that has no financial impact – its impact is likely to come in the form of damage to credibility or reputation which can destroy enterprise value.
- A company's "risk profile" should not exceed its "risk appetite".
- Responsible companies should disclose to stakeholders the nature and levels of risk associated with the lines of business in which they are engaging.
- Companies should adopt risk management policies which deal with financial and non-financial risk, are understood throughout the organisation and the associated process is accepted by all management as a "performance enhancing" activity for the business.
- Companies should adopt systems and processes that deal with difficult "or grey areas", which will effectively identify and manage non-financial risk and which can quickly inform the board of the big picture (such as, risk management cycles, heat maps etc).
- Stakeholders in the enterprise should receive from the enterprise sufficient information on policy and process to assure them that this is the case.

The Role of Corporate Counsel in Identifying and Managing Non-Financial Risk – the Value Add

- Many of the most material risks facing large public corporations today are "non-financial" risks.
- These include geo-political, compliance, regulatory, reputational and societal risks.
- The assessment and mitigation of such risks calls for the application of a wide range of law, regulation and (often) opinion, together with a substantial degree of "real-world" business experience.
- Corporate Counsel must be appropriately positioned in the organisational hierarchy, "break out" of conventional stereotypes of their role and supplement their legal education with risk management training.

Remediation of Non-Financial Risks

Once identified non-financial risks must be effectively managed and remediated including:

- Immediate corrective action (including any compliance and governance issues).
- Update policies and procedures and obtain buy-in throughout the whole organisation.
- Address cultural and behavioural issues (openness, tone from top).
- Effective Oversight and Assurance.
- Total Performance.