NAO EXPERIENCE OF IT GOVERNANCE REVIEWS

ADAPTED FROM NAO TRAINING MATERIAL 2007

The UK National Audit Office (NAO) has begun (since 2003) to carry out discrete reviews of the IT functions in some of its clients, major UK Government Departments. These reviews have focussed on the top level organisation of IT and on how Departments use and manage those systems. So far the output of these reviews have been management reports, confidential to the Department, although the NAO may consider publishing a summary of the findings from a series of such reviews in the future.

Why do the NAO get involved?

The NAO's financial audit methodology requires us to consider governance issues as part of the audit planning process "understanding the business" and this work may inform an IT Governance review and particularly identify suitable areas for and timing of investigation. However, the NAO does not conduct IT Governance reviews as a matter of routine. These reviews are discrete pieces of work, undertaken with the active cooperation of the Department concerned and have a discrete output, a management report.

What is IT Governance?

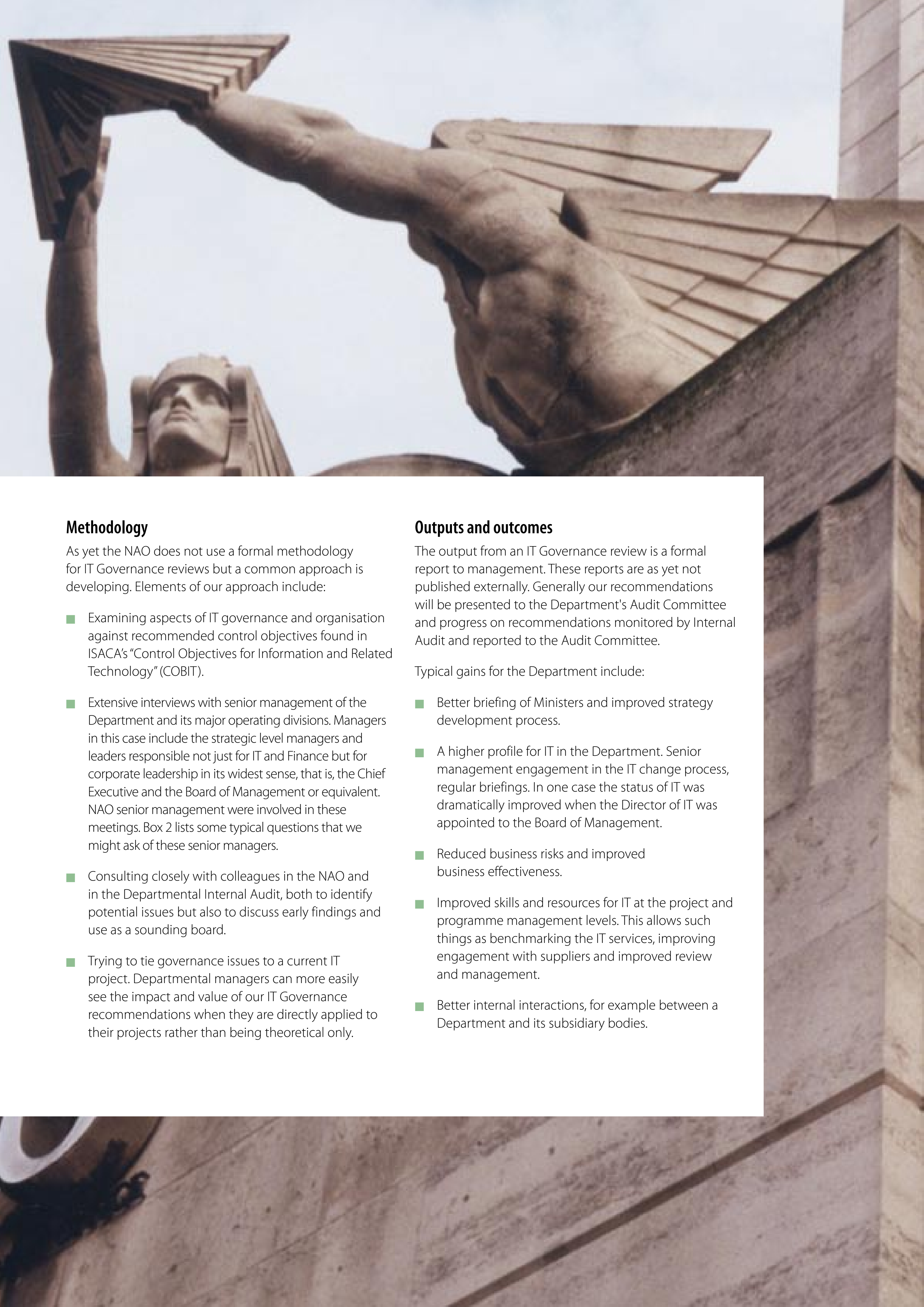
The IT Governance Institute (part of ISACA) defines IT Governance as "an integrated part of Corporate Governance. It is the responsibility of the board of directors and executive management and consists of the leadership and organisational structures and process that ensure that the organisation's IT sustains and extends the organisation's strategy and objectives."

There are general triggers for carrying out an ITG review:

- Many Departments rely on IT to support the change process and provide efficiency savings. They have invested heavily in IT in the past and plan to continue with serious investments
- Governance plays an important role in the success of IT projects. In particular the NAO has identified a number of cases where poor governance has been a contributory cause of project failure. For examples see the NAO's composite report "Delivering successful IT-enabled business change" published in November 2006 (http://www.nao.org.uk/pn/06-07/060733.htm).

Particular reasons for carrying out an ITG review at a specified Department might include

- The emergence of IT issues in a Department that has already had its share of IT failures.
- Governance weaknesses being identified in Gateway reviews on developing projects – see http://www.ogc.gov.uk/what_is_ogc_gateway_review.asp for general background on this scheme. The National Audit Office found in their analysis of Gateway reviews that 43% of reviews highlighted the need to strengthen project management.
- Key components of IT Governance missing, for example an up to date strategic plan for IT, identified perhaps as part of the financial audit.



Methodology

As yet the NAO does not use a formal methodology for IT Governance reviews but a common approach is developing. Elements of our approach include:

- Examining aspects of IT governance and organisation against recommended control objectives found in ISACA's "Control Objectives for Information and Related Technology" (COBIT).
- Extensive interviews with senior management of the Department and its major operating divisions. Managers in this case include the strategic level managers and leaders responsible not just for IT and Finance but for corporate leadership in its widest sense, that is, the Chief Executive and the Board of Management or equivalent. NAO senior management were involved in these meetings. Box 2 lists some typical questions that we might ask of these senior managers.
- Consulting closely with colleagues in the NAO and in the Departmental Internal Audit, both to identify potential issues but also to discuss early findings and use as a sounding board.
- Trying to tie governance issues to a current IT project. Departmental managers can more easily see the impact and value of our IT Governance recommendations when they are directly applied to their projects rather than being theoretical only.

Outputs and outcomes

The output from an IT Governance review is a formal report to management. These reports are as yet not published externally. Generally our recommendations will be presented to the Department's Audit Committee and progress on recommendations monitored by Internal Audit and reported to the Audit Committee.

Typical gains for the Department include:

- Better briefing of Ministers and improved strategy development process.
- A higher profile for IT in the Department. Senior management engagement in the IT change process, regular briefings. In one case the status of IT was dramatically improved when the Director of IT was appointed to the Board of Management.
- Reduced business risks and improved business effectiveness.
- Improved skills and resources for IT at the project and programme management levels. This allows such things as benchmarking the IT services, improving engagement with suppliers and improved review and management.
- Better internal interactions, for example between a Department and its subsidiary bodies.

The NAO has gained:

- Better understanding of departments, which feeds back into our financial and performance audit work with departments.
- Positive reaction from departments and their Audit Committees. This has increased the NAO's profile with them, and improves our client relationship.

Lessons learnt

The results of the IT Governance reviews carried out so far have been very positive, with departments welcoming our recommendations and actively pursuing resolution of problems we have identified.

- IT Governance reviews do not have to be carried out by specialist IT auditors with IT technical skills. Rather they should be carried out predominately by audit staff with a good knowledge of good practice in IT Governance. In the NAO IT auditors and IT specialists have been used to advise the audit teams.
- Reviews can usefully draw on existing corporate knowledge, gained from financial or performance audit work.
- Any failed IT project has implications for IT Governance.
- The finished product can increase the NAO's profile with the Department.
- These reviews place a premium on sensitive management of client / NAO relationship. We need to capture the views of very senior staff and it is important to pitch questions at the right level.

Questions for Senior Management

A Senior Management Leadership and Strategy

- Is there sufficient awareness of IT issues at Ministerial level?
- Is there sufficient visibility of IT issues at Departmental Management Board level?
- Is there sufficient skill and expertise at Board level to exercise oversight of major IT enabled projects and programmes?
- Is there an IT strategy aligned to business in place to enable the Board to make appropriate decisions in a timely manner?
- In making investment decisions was the Board able to consider the portfolio of projects, its risks, interdependencies, benefits, capability to manage the programme.
- Where projects and programmes traverse organisational boundaries is there a clear understanding of risks and interdependencies?

B Management of Risks and Realisation of Benefits

- Are risks identified and managed and benefits identified and realised at the project level?
- Is the role of Internal Assurance Department effective?
- Is the Department effectively participating in Gateway reviews?
- Has the Department a means of ensuring that emerging lessons are being learned across projects and programmes?

C Stakeholder and supplier engagement

- Does the IT Department maintain effective customer liaison?
- Does the IT Department provide strategic technical input?
- Does the Department have effective communication with suppliers?
- Is the Department commercially aware?
- Is the Department effectively managing its suppliers?

D Programme and Project management

- Are there appropriate policies and guidance?
- Are the Senior Responsible Owners (SRO) appropriately skilled?
- Are members of the Programme and Project Boards appropriately skilled?
- Is the performance of the IT Department being managed effectively?
- Is an IT Governance Tool being used?