Key Success Factors for Implementing IT Governance

Let’s Not Wait for Regulators to Tell Us What to Do

By Erik Guldentops, CISA, CISM

The realisation that IT is so pervasive in the business environment and so critical for the success and survival of enterprises has resulted in IT being placed on the agenda of boards and executives. Further, it has ensured that IT has become an item of interest and concern within the broader scope of corporate strategy and governance.

There is no denying that an efficient and effective information infrastructure can enhance shareholder value. Conversely, IT failures do affect the image and reputation of enterprises in the increasingly interconnected economy.

The financial sector took the lead in establishing best practices for governance and control over IT, closely followed by the telecommunications industry—even before the emergence of the regulations on operational risk (Basel II). However, those initiatives may be overtaken by the reaction to major corporate wrongdoings, like Enron and WorldCom.

As a result, regulation relative to internal control and assurance is significantly expanding. These regulations—Sarbanes-Oxley in the US and similar developments in other countries and within international professional bodies—are building on earlier regulations, including Turnbull in the UK, which set standards for internal control and risk transparency for companies listed on the London Stock Exchange.

It will be interesting to see how strongly IT will be positioned in upcoming regulatory requirements for internal control and governance, but that should not stop us now from looking at some of the key success factors for control and governance of IT:

1. **Forming IT strategy and IT steering committees**—The IT strategy committee operates at the board level, providing direction to IT strategy and ensuring it is aligned to the business strategy, while monitoring how management delivers against that strategy. The IT steering committee operates at the executive or senior management level, driving IT priority setting and resource allocation, while continuously monitoring the success of, and value returned by, major IT initiatives. The role of both committees has been expanding over the last couple of years as awareness of IT governance has grown. They have fostered an essential increase of business participation in decisions about strategic direction, investment priorities, sourcing and optimisation of IT.

2. **Aligning IT and the business in strategy and operations**, even to the extent of establishing business/IT relationship managers and making the business and IT co-responsible for the commercial and technical success of IT projects.

Foremost in this alignment is the integration of business and IT strategy. It is hoped that the statistics shown in several 2002 surveys improve. Their results showed that, on average, one-quarter of enterprises had no business strategy, one-quarter had a business strategy but no IT strategy, one-quarter had separate business and IT strategies, and one quarter had an integrated strategy.

3. **Cascading of IT goals and strategy** down into the organisation, translating them for each layer in the organisation while linking them to a simple but effective measurement system that feeds performance results up the organisation. Again, surveys in 2002 did not paint a pretty picture, reporting that the linkage deteriorated rapidly when going into the organisation.

4. **Applying emerging management best practices** that focus on value delivery:
   - Standardisation of technology, including centralisation of IT staff; the use of technology “czars” and technology councils or review boards to establish and monitor standards and architecture
   - Disciplined project management with a sponsor role for the business, frequent stakeholder meetings and management accountability for business outcomes
   - Value clarification with metrics to capture costs, benefits and progress toward achieving expected value

5. **Implementing a governance and control framework for IT**—Implementation decisions made by enterprises taking a lead in IT governance, choices by regulators and commentaries by major market analysts confirm over and over again that Control Objectives for Information and related Technology (COBIT) is a reference framework of choice. Its complete mapping to COSO I and its successor, Enterprise Risk Management (ERM), is further evidence.

COBIT is well accepted, though not advertised, by many enterprises. It is primarily introduced by the audit function as the auditors’ framework for judging control over IT. However, audit committees are starting to ratify it as an audit standard, and regulators have begun to refer to it or adopt the content in their own developments. Most importantly, IT groups have picked it up, often because it provides for performance measurement. COBIT appears complex to some and emerges as quite a challenge for others, calling for extensive implementation skills. But then, following the bursting of the techno bubble, the downturn of
the economy and (although perhaps a minority view) the apparent reduction of IT’s strategic importance, the world of IT has a lot of catching up to do relative to what is considered good practice in controlling and governing IT.

COBIT does provide the basis and the tool set to analyse—based on the enterprise value and risk drivers—where the enterprise is relative to IT governance and where it needs to be. That leads to a gap analysis and the identification and prioritisation of control improvement initiatives. The recently published IT Governance Implementation Guide, which uses COBIT and provides a road map with detailed process steps and tools, makes the analysis and planning process a lot easier.

Alignment, transparency and measurement supported by a control framework are the key factors for success in governing IT. Aligning business and IT will improve the strategy direction and ensure better delivery against the strategy. Performance measurement will support management’s and the board’s control responsibilities. This will reduce risk and produce better value for money from IT—two fundamental corporate governance responsibilities.

Sarbanes-Oxley significantly raised top management’s responsibility relative to financial reporting and internal control. The stakes are further raised with requirements on speed and extent of reporting and the debate on what standards form the basis for internal control. It is clear that IT plays a major role in financial reporting and internal control. It is equally apparent that IT governance must be the foundation for reliability of reporting and effectiveness of the system of internal control in the global, dematerialised economy. Let us, therefore, get started on some of these best practices before regulators tell us on which ones need to be reported.

**Endnotes**

1. Acadys and the Hunter Group
2. Practices Survey, CIO Insight, Special Issue 2002

**Erik Guldentops, CISA, CISM**
is advisor to the board of the IT Governance Institute and an executive professor in the Management School of the University of Antwerp, Belgium, where he teaches on the subjects of IT security and control, IT governance and risk management. In 2001, he retired as director of security of SWIFT, where he also previously held the position of chief inspector. He initiated and has headed the development of COBIT since the early 1990s and currently is chair of ISACA’s COBIT Steering Committee.