IT and Enterprise Governance

By Michael J. A. Parkinson, CISA, CIA, and Nicholas J. Baker, CPA

Enterprise Governance

Enterprise governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.[1]

This definition, outlined by the IT Governance Institute (ITGI) has been widely adopted and forms a sound basis for a broader discussion of IT governance. It is important to distinguish between governance and management, and the definition makes it clear that there is at least a point of contact if not actual overlap. The need for formal governance processes arises when those who are in control of the assets of an organisation (management) are not the owners of the organisation. The owners or principal stakeholders appoint individuals (the board) to guide the organisation on their behalf. These individuals, working with top management, establish governance processes to ensure the effective delivery of organisational objectives.

Enterprise governance is largely about frameworks and processes. It is the way in which decisions are made and outcomes monitored. Organisational management are stewards of the resources of the organisation on behalf of its owners; the board guides and monitors the activity of organisational management as representatives of the owners.

When working well, [an enterprise] governance framework produces better outcomes simply because it exists.[2]

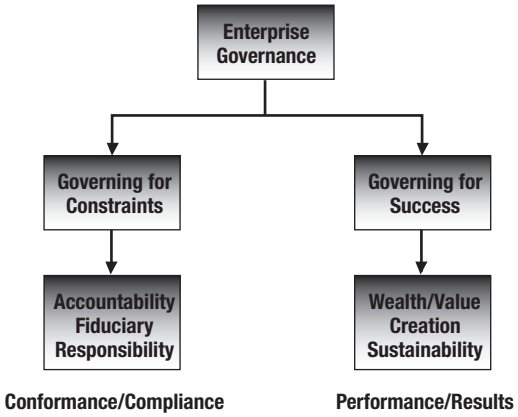
What This Means in Practice

Recent research[3] has illustrated that governance has two equally important aspects—doing the right thing (driving performance) and doing things the right way (ensuring conformance). An organisation will not remain healthy by simply complying with law and good business practice, but without this compliance, it is very likely to fail. This is illustrated in **figure 1**.

There is some value in using this model to think about the role of information technology in an organisation. IT can contribute to both aspects of governance: it can improve performance and aid compliance.

Well-governed organisations establish processes with the objective of achieving, first, the purpose for which the organisation was established and, second, the requirements of legislation and regulators.

Figure 1—Enterprise Governance Model



Control Frameworks and Legal Compliance

Established control frameworks, such as the Committee of Sponsoring Organisations (COSO) or COSO Enterprise Risk Management (ERM), provide a structure in which good governance can be implemented. The control environment of an organisation is driven by the attitude taken at the top of an organisation in relation to performance demands and conformance imperatives. Organisations that emphasise performance at the expense of compliance (both legally and ethically) have been the origin of many scandals. However, organisations that emphasise conformance at the expense of performance may become lethargic and inflexible.

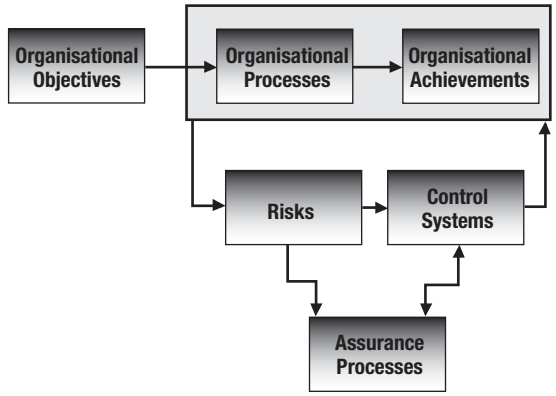
These frameworks also place risk assessment or risk management in a central position. Risks exist in relation to both aspects of the governance framework, and appropriate control systems must be put in place to address those risks. These risks, according to COSO,[4] are in relation to the following broad objectives:

- Economy and efficiency of operations, including achievement of performance goals and safeguarding of assets against loss
- Reliable financial and operational data and reports
- Compliance with laws and regulations

The assurance processes established within an organisation have a three-fold responsibility, as illustrated in **figure 2**, to examine the control systems in relation to the risks and achievements of an organisation to ensure that those controls are:

- Adequate to the risks
- Effective in operation
- Efficient

Figure 2—Objectives, Risks, Control and Assurance



The legal constraints placed upon organisations by such legislation as the US Sarbanes-Oxley Act or the Health Insurance Portability and Accountability Act (HIPAA) do not add anything beyond addressing these risks. The legislative framework exists primarily to protect the stakeholders of the organisation. It very often provides minimum performance levels in relation to risks that would ordinarily arise in the course of running a business.

An Integrated Governance Model

Boards have a responsibility to establish mechanisms and monitor operations to ensure that organisations achieve their objectives and comply with the law. This monitoring covers the operation of control systems and accuracy of reporting. Aspects of the monitoring function are frequently delegated to an audit committee.

The audit committee has three sources it can use to obtain the assurance it needs. It can enquire of line management, which have primary responsibility for delivery of the organisation's outcomes, or it can enquire of the internal or external auditors. These three groups each provide incomplete information, but they provide it from different perspectives, so the audit committee may be able to construct a complete picture from independently sourced information from those groups.

Organisations set up many assurance functions (e.g., quality assurance groups, complaints systems, risk management groups and internal auditors) and have others imposed upon them (e.g., external auditors, regulatory inspectors). The audit committee is entitled to consider the reports of each of them in coming to a conclusion about the operation of an organisation.

The assessment and management of risk is the centrepiece of the governance model. Risks arise because of corporate objectives. These risks must be held to acceptable levels by control (treatment) regimes. Assurance processes are established so that the board can confidently monitor the management of risks and the achievement of organisational objectives (**figure 3**).

IT Governance

Logically, IT governance is a subset of enterprise governance. IT governance covers performance and compliance considerations. Since IT is an enabler to business, perhaps it is fair to say that IT governance exists to help organisations make the most of IT.

> *IT governance…is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives.*[5]

Practical Implications

This definition implies that IT governance has three components:

- Leadership—Suggesting vision, responsibility and accountability
- Organisation—Suggesting staffing, resourcing and structures
- Processes—Suggesting established standards and procedures

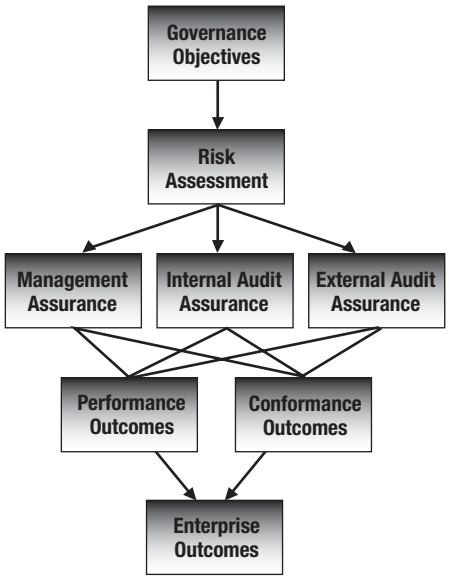
Each of the *Control Objectives for Information and related Technology* (COBIT) domains can be analysed in these terms, thus providing valuable practical insight into setting up and running an IT function.[6] A full discussion of this is beyond the scope of this article.

The IT Governance Institute's *Board Briefing on IT Governance, 2nd Edition*, expands the above definition and describes IT governance as also:

- Setting strategy
- Delivering value
- Measuring performance
- Managing risks

Importantly, this expanded definition encompasses the management of risk—specifically, risks that arise in relation to strategy, risks in relation to delivering value, and risks in

Figure 3—Governance Frameworks

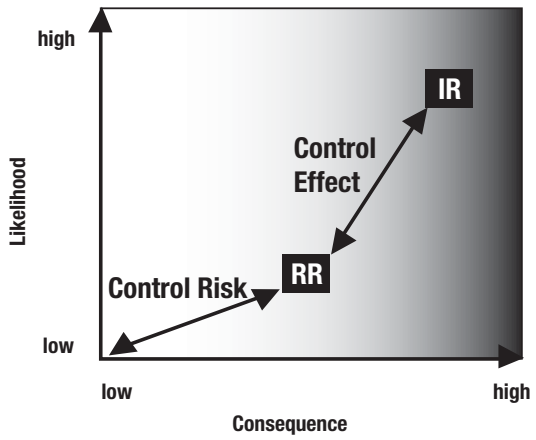


relation to measurement and reporting. The bottom-line questions for IT governance are:
- Do the systems support the business?
- Do the systems comply with law and regulation (security, privacy, health and safety)?
- Do the systems provide accurate results?

IT Risk Assessment

The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets. The impact or relative severity of the risk is proportional to the business value of the loss/damage and to the estimated frequency of the threat.[7]

Figure 4—Risk Model



While there are many IT risk assessment techniques, they all are mechanisms for identifying events that may affect objectives, the potential consequences of those events and the corresponding likelihood of those occurrences. The result of a risk assessment is a prioritised list of possible events that can form the basis for further action. **Figure 4** illustrates the ranking method. Higher priority risks are toward the upper right corner of the chart.

IT risk assessment requires knowledge of the vulnerabilities of technology, the potential failures in computer systems implementations and the corresponding business implications.

Three types of risk are of interest:
- Inherent risks—The risks present in the normal course of conducting business
- Control risk—The risk that controls will not prevent, correct or detect an adverse event
- Residual risks—The risks after controls are taken into account

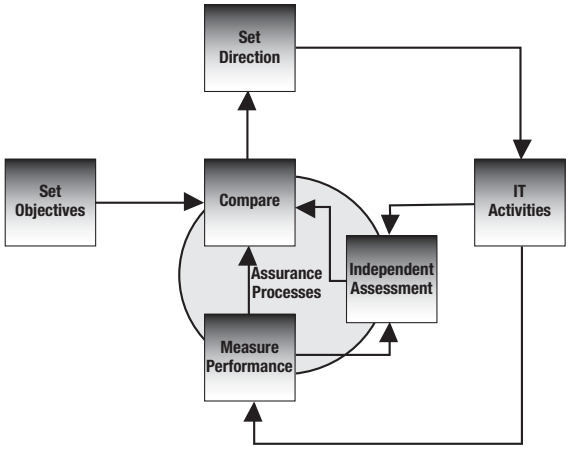
The board's primary interests in these risks are that there is a systematic method of identifying and assessing them, the organisation's risk tolerance has been taken into account in determining appropriate treatment and the prescribed treatments are functioning as intended. Some risks might be of such magnitude that the board requires routine reporting against them. Day-to-day management processes will handle the majority of risks.

Key questions to ask are:
- Is the residual risk associated with each possible event acceptable to the organisation?
- In those circumstances where there is a serious inherent risk, is the control risk acceptable?

IT Assurance

These questions form the basis of the IT assurance that boards require so they can fulfil their IT governance obligations. Assurance is based on information. Assurance processes provide information—either direct representations of performance or corroboration of such representations. **Figure 5** adapts a diagram from *Board Briefing on IT Governance,* 2nd Edition*,* to illustrate the place of IT assurance in the governance framework.

Figure 5—IT Assurance

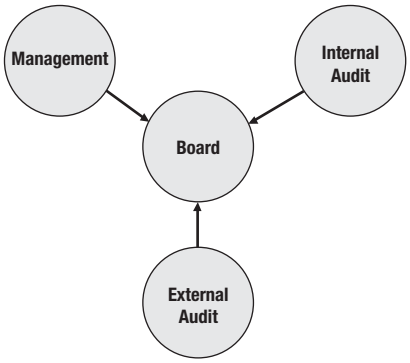


Sources of Assurance

As suggested earlier, boards/audit committees seek assurance from a range of sources. The bulk of the information they use in making decisions comes from organisational management itself. Organisational management have the best access and the most extensive resources; therefore, they can provide the best information. Management information is expert, but it is not independent of the operations. Management information is useful but may not be balanced, so boards are forced to look beyond management representations to independent advice, which is generally obtained from a range of IT auditors (both internal and external to the organisation).

The quality of corporate governance depends upon the quality of information that is at the boardroom table and the intellectual honesty applied by directors. Both of these are needed if a board is to function effectively.[8] Ensuring that information is received from multiple mutually independent and properly qualified individuals provides structural encouragement for boards to obtain the best quality information. Experience has established that boards generally require at least three mutually independent sources of assurance (see **figure 6**).

Figure 6—Governance Information Sources



IT Management

The front line in risk management in any organisation is line management. The front line in addressing IT risks is IT management. An increasing number of IT managers are structuring and managing their organisations consistent with COBIT. COBIT forms a sound basis for establishing responsibilities and measuring performance. While this is useful to auditors, it can be extremely valuable to IT management. IT management can establish a level of performance appropriate to the needs of their organisation and can report against it.

The knowledge that the IT function is appropriately focused can provide important assurance to the board. It will know that the IT function is striving toward the most appropriate practice for the organisation.

IT Security

IT security relates to the protection of valuable IT assets against loss, misuse, disclosure or damage.[9] It is a critical control within an IT governance framework. IT security systems address a wide range of risks in the conformance and performance arms of the model. A well-structured IT security function, staffed with appropriately qualified individuals, forms the foundation for high-quality performance in this area and is the basis for positive assurance to the board.

Greater assurance will be provided should the IT security function be certified against BS 7799-2.[10] This standard forms a basis for a complete IT security management process.

IT Audit

These management functions provide valuable assurance to the board, but both are incomplete information. The information provided by IT management will be balanced by the information provided by the independent assurance functions: the internal or external auditors.

The IT assurance function will examine the performance of IT management and IT activities (including IT security) against appropriate standards [such as COBIT, IT Infrastructure Library (ITIL), ISO 17799 and BS 7799-2]. The independent information provided by IT assurance provides confidence to the board.

On an important issue (e.g., in relation to the accuracy of financial reporting), it is reasonable for the board to receive advice from all three arms of the assurance process: management, internal audit and external audit.

Reporting

Three streams of reporting to the audit committee correspond to the three streams of assurance. Assurance is routine information from management, confirmation (or exception) information from the internal auditors and specific financial reporting information from the external auditors. An audit committee will expect to see an internal audit programme balanced by external audit review and management assurance, and IT assurance filling an appropriate place in those programmes.

The audit committee will want to see reports of IT security and IT management activity as they relate to the significant risks of the organisation. They will want these reports to be complemented by reports from the auditors. When the auditors believe that controls can or should be improved, the audit committee will expect to see an appropriate response from management.

Only organisational management can implement controls; the auditor's role is to assess and report. Generally, the audit committee obtains assurance that the agreed-upon action has been undertaken by asking the internal auditors to track and report action on recommendations, although it is not unusual for an audit committee to invite responsible managers to meetings so they may report in person.

Conclusion

IT governance is an integral component of enterprise governance, just as IT is integral to modern organisations. IT governance must address issues of performance (value generation) and conformance (regulatory compliance). A governance framework requires a process of reporting actual performance—assurance that processes put in place are working as expected.

IT functions may adopt a range of standards as a basis for delivery of services to their organisation, but IT service objectives remain the same—to promote the success of the organisation. IT managers must consciously consider conformance and performance—that is, they must address all the risks that are relevant to IT service delivery.

IT auditors, whether external or internal, complement the activity of IT management and IT security professionals by providing independent confirmation of the accuracy of management representations and through their own assessment of the IT activities and achievements.

Endnotes

[1] IT Governance Institute, *Board Briefing on IT Governance*, *2nd Edition*, 2003, p. 6. This definition was adopted in the CIMA paper cited below.

[2] Uhrig, John; "Review of the Corporate Governance of Statutory Authorities and Office Holders", Commonwealth of Australia, 2003

[3] Chartered Institute of Management Accountants, *Enterprise*

Governance, 2004, *www.cimaglobal.com*. The CIMA diagram has been modified by the authors for the purpose of this article.

[4] Committee of Sponsoring Organisations, Internal Control—An Integrated Framework, 1992

[5] *Op. cit.*, IT Governance Institute, *Board Briefing on IT Governance*, p. 10

[6] We are indebted to a contribution from Randy Lawton on the IT governance listserv for this insight.

[7] International Organisation for Standardisation, *Guidelines for the Management of IT Security*. An equivalent definition can be found in Australia/New Zealand Standard AS/NZS 4360 Risk Management: 'The chance of something happening that will impact upon objectives. It is measured in terms of consequences and likelihood.'

[8] King, Mervyn E; IIA International Conference, Las Vegas, Nevada, USA 2003

[9] IT Governance Institute, *Information Security Governance: Guidance for Boards of Directors and Executive Management*, 2001, p. 8

[10] This British Standard has been republished as an Australia/New Zealand Standard (AS/NZS 7799.2). It is the second part of a two-part standard. Part 1 of the standard has been adopted as ISO 17799.

Michael J. A. Parkinson, CISA, CIA
is a computer programmer turned internal auditor. He has more than 20 years of experience in internal auditing and currently is a professional services provider at KPMG in Canberra, ACT, Australia. He is past president of the ISACA Canberra Chapter and was an international vice president of ISACA from 1994-1997 and 1999-2000. He is currently chair of the ISACA Education Board. He has written a number of publications and has guided teams of authors in the production of a number of professional guidance publications for internal auditors.

Nicholas J. Baker, CPA
is a partner in KPMG Canberra. Baker has 20 years of experience in IT auditing after an initial career in IT. He has been a prominent advisor to the Australian government in governance and control matters and is responsible for a range of internal and external audit activities.

Information Systems Control Journal, formerly the IS Audit & Control Journal, is published by the *Information Systems Audit and Control Association*, Inc.. Membership in the association, a voluntary organization of persons interested in information systems (IS) auditing, control and security, entitles one to receive an annual subscription to the *Information Systems Control Journal*.