Make Sure Management and IT Are on the Same Page: Implementing an IT Governance Framework

By Gary Hardy
ISACA Journal Volume 3, 2002

Do any of these conditions sound familiar?

- Increasing pressure to leverage technology in business strategies
- Growing complexity of IT environments
- Fragmented IT infrastructures
- Demand for technologists outstripping supply
- Communication gap between business and IT managers
- IT service levels that are disappointing
- IT costs perceived to be out of control
- Marginal ROI/productivity gains on technology investments
- Impaired organisational flexibility and nimbleness to change
- User frustration leading to ad hoc solutions
- IT managers operating like firefighters

IT is one of the most significant functions within an organisation, yet can be one of the most difficult and frustrating areas to manage. IT is known to be a challenging and rapidly changing area, full of uncertainty and risk, as well as opportunity and almost unlimited potential. And it is not surprising that top management find it difficult to understand and influence the way IT can best serve the interests of the business. But, with common sense and good management practices, much can be done to improve the overall performance of IT and reduce the number of failures and disappointments.

Companies that have been successful with their IT often share a common theme--the business side is involved and committed to what IT does. They are engaged in all IT activities, run their operation with IT involved in every aspect of business planning and, most importantly, priorities, commitments and risk management are shared responsibilities, not disjointed management activities. In cases where IT has been outsourced, it has been most successful when management has maintained control through the use of good service level agreements and effective monitoring. When there is a joint and shared responsibility between the customer and the provider, there usually is a better outcome.

If IT is to deliver the services that a business needs now and in the future, it has to be managed by the business as a whole. This is what IT governance is about. IT governance is a topical subject but perhaps not well understood. In simple, practical terms it means making sure that those responsible for running an organisation--the board of directors--are able to exercise effectively responsibility over the use of information technology just like any other part of the business. It does not mean autocratic rule or one-sided monitoring. It means a way of running the organisation so that risks are managed and the interests of all stakeholders are covered.

The IT Governance Institute's COBIT materials provide an excellent framework and common language for everyone in an organisation to view and manage IT activities. Incorporating a single culture and operational model and a common language for all parts of the business involved in IT is one of the

most important and initial steps toward good governance. It also provides a framework for measuring and monitoring IT performance, and the COBIT *Management Guidelines* provide an excellent basis for doing this.

Recognising why it is important to manage IT risks and implement a governance framework and then how to create a culture whereby everyone works with IT as a team, rather than as disparate groups, is the next key step. The *Board Briefing on IT Governance*, published by the IT Governance Institute, sets out an excellent explanation of how to do this and provides useful tools to help get started. It covers:

- What is IT governance?
- Why is IT governance important?
- Who does it concern?
- What can be done about it?
- What does it cover?
- What questions should be asked?
- How is it accomplished?
- How do organisations compare?

This article provides a further dimension. It will help one recognise the practical issues that regularly concern top management, so that when the governance process is being implemented, the organisation can ensure it provides answers to the kinds of questions increasingly being put forth at senior management meetings. It will help auditors put themselves in the shoes of top management--appreciating and anticipating what ought to be governed effectively. So, IT auditors, IT consultants, IT practitioners and IT managers will have an insight into the wider management issues that a good governance scheme should cover.

And a good test of an IT professional's ability to govern IT within the organisation is to consider how well the issues in the following areas are understood and approached.

To govern IT effectively, it is important to appreciate the various activities and risks within IT that need to be managed. Using the COBIT *Framework's* four domains--Planning and Organisation, Acquisition and Implementation, Delivery and Support, and Monitoring--it is possible to look at this logically from a top management perspective.

Planning and Organising

Are IT and the business strategy in alignment?

One of the biggest challenges facing most companies today is making sure that the business and IT are moving in the same direction. IT strategy in the modern IT world can have many different interpretations due to the speed of change in IT and the increasingly short timescales businesses expect from IT developments. But if top management cannot articulate where IT fits into the corporate plan and how IT is going to enhance corporate efficiency and competitive advantage over the next year, then they are not governing this key area.

Is the enterprise achieving optimum use of its resources?

IT resources--both people and technology--are key ingredients of a successful IT operation. Manpower costs account for about half the IT expenditure in an average organisation (based on Gartner analysis), yet acquiring the right skills and then applying those skills to the maximum effect can be difficult. Management should know what level of competency exists and whether it is adequate to support planned IT activities, and they also should be in a position to measure manpower productivity and effectiveness.

The effective use of existing technology is important, otherwise costs will be excessive and business functions will not benefit from IT. Management need to be aware of user satisfaction levels and should measure things like level of standardisation, age of technology and maintenance costs to reveal the technology's effectiveness.

Leveraging new technology developments is a risky area and organisations must decide whether to be at the leading edge, up-to-date with current technical developments or safely following the pack. If the IT function is not following the risk profile with which the business is comfortable, then there is a risk of failure ahead.

Does everyone in the organisation understand the IT objectives?

This is all about communication and feedback, backed up by clear and consistent objectives. Management should be able to build a culture throughout the organisation and set objectives in IT and business areas that are consistent and complementary so everyone understands their role and responsibilities with respect to IT systems. If management cannot measure how this is being achieved, they are not governing the execution of the IT plan.

Are IT risks understood and being managed?

Risks relating to IT are more significant than they used to be because organisations are more vulnerable to problems due to the inherent nature and complexity of IT and also because the impact of a failure can have much higher consequences.

Management must set the risk management policy and should be aware of how that policy is being executed. From time to time, they should seek reassurance from internal audit and external reviewers that any significant risks--whether security-related or related to a major new project--are being managed properly.

If there is uncertainty over who has risk management responsibility or if there is a pattern of unexpected failures and incidents, this area probably is not being governed properly.

Is the quality of IT systems appropriate for business needs?

Quality control in IT can be something easily delegated to the specialists. However, quality control is a basic principle that needs to be aligned with real business needs. The quality of the IT systems must fit the purpose for which IT is being used.

Management should set the right level of quality expectation and follow this through with quality sign-off and appropriate approvals. They should be aware of any significant deviations from quality plans and should support a quality assurance framework appropriate for the needs of the business.

Acquiring and Implementing New Systems

Are new projects likely to deliver solutions that meet business needs?

This is all about matching IT opportunity to business needs. It is a two-way and joint, team-based process. Top management needs to be involved in the choice of projects and strategic direction. But they are unlikely to be involved closely in the projects themselves. They can, however, monitor the effectiveness of the team, ensure there is adequate involvement of all the right players and measure progress to ensure outcomes are likely to be successful. They also can challenge the approaches taken, question whether the right resources are being used, question whether external help is needed and place responsibility on management for ensuring that solutions are meeting the needs of their business area.

Are new projects likely to deliver on time and within budget?

New IT projects can result in high costs and a dependency on IT to meet commercial deadlines and operational plans. Increasingly, time-to-market and time-to-delivery in IT are getting shorter and shorter. Management must ensure that the goals set are realistic and do not put the whole business at risk, must identify projects that are most important to succeed and must identify when and where projects are going wrong. They should insist on effective project risk management and project monitoring and be prepared to intervene when needed.

Will the new systems work properly when implemented?

This is dependent on the use of adequate and thorough testing and authorisation procedures when new systems are being introduced. Top management never will be involved in the detail of these activities, but they can influence the pressure exerted by the business on IT to rush implementations; make sure--especially for business critical systems--that tests have been completed, proven and approved; make business functions accountable for acceptance and, where necessary, seek third-party confirmation that the systems are working as intended before going live.

Will changes be made without upsetting the current business operation?

One of the biggest dangers with today's complex and networked systems, involving many IT players (in-house as well as service providers), is the increased probability that a minor unintended error can inadvertently cause systems to crash. Strict controls need to be enforced by top management that forbid uncontrolled or untested changes and ensure that access to production systems is carefully safeguarded.

Service Delivery and Support

Are IT services being delivered in line with business priorities?

IT is an integral part of the day-to-day business operation, automating and providing support to nearly all of the business processes and functions within the organisation. Therefore, the IT systems need to be reliable, secure and available when needed (which increasingly is all of the time). For many processes, this can mean high levels of service and dependency on IT to operate. Management should insist on properly defined services and service level agreements and that they be monitored and measured in terms understandable to the business.

Are IT costs optimised?

All businesses need to manage their operations within reasonable costs, and IT, like any other part of the business, must strive for the lowest operating costs and the most efficient service. The operational cost base for IT is probably more complicated than any other part of the business infrastructure and needs to cover all the technology costs (hardware, software, communications networks, etc.), the manpower-related costs and the costs of suppliers and a growing number of external service providers. The IT cost base is much more dynamic and fast-changing than nearly any other area, so it needs to be managed proactively, if costs are to be optimised.

Is the work force able to use the IT systems productively and safely?

Even the best IT systems succeed or fail depending on the effectiveness of their users. Management should measure levels of user satisfaction, the amount of training users receive and the level of support needed. They also should watch the trends in these areas, driving for continuous improvements.

Are adequate security, integrity and availability in place?

It is ultimately top management's responsibility to ensure there is an adequate control environment around information, one of the organisation's most valuable assets, as well as the information systems themselves. They should verify on a regular basis that the control framework is functioning properly, use internal and external auditors to verify compliance with key controls and insist on an appropriate control culture within the organisation.

Monitoring

Can IT's performance be measured and can problems be detected before it is too late?

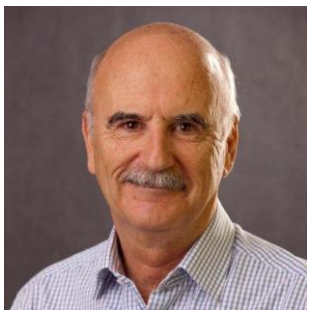
Management should have in place a set of metrics that gives them a regular and accurate view of how IT is performing for ongoing operations and for new projects. Operating without such measures is like driving a car with a blacked-out windshield and no instruments. The metrics must be business-oriented, not technical measures, and ideally based on agreed service levels and service definitions. This is especially important when external service providers are used.

Is independent assurance needed to ensure critical areas are operating as intended?

Management should, in conjunction with an audit committee, determine the extent of internal and external independent assurance required. There are several areas within IT where this is good practice, for example, security, regulatory and legal compliance and any specifically high-risk areas. Independent input is a key ingredient of good governance, including periodic assessment of the governance process itself.

-x-

For more information on this article or the author, please visit www.itwinners.com



For this publication, Gary Hardy was awarded the ***Michael Cangemi "Best Article / Book Award"***, to recognise his outstanding contributions in technical publishing.

Gary Hardy
Director, IT Winners CC
082 857 0727
gary.hardy@itwinners.com