FEATURE

Principles of Governance
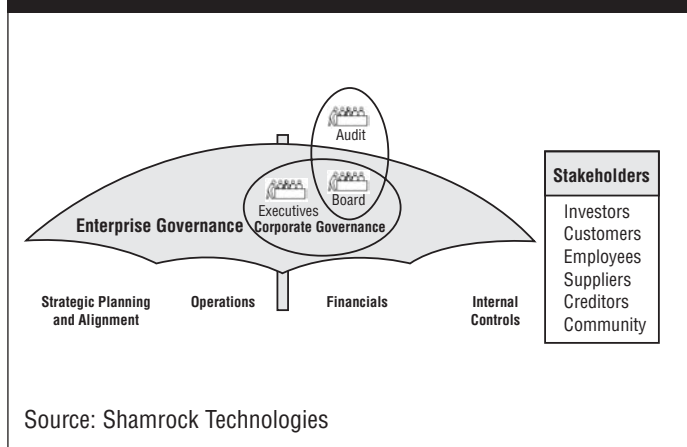
By Stacey Hamaker, CISA, and Austin Hutton

This article describes the common characteristics of well-governed organizations and enables readers to apply these characteristics to their own organizations. This article draws from the multiple aspects of governance found in:

- Enterprise governance
- Corporate governance
- Information technology (IT) governance

The material in this article is an extension of that found in an article published in volume 1, 2003 of the *Information Systems Control Journal*, "Spotlight on Governance."[1] The original article provides an overview and definitions[2] of the three forms of governance, a comparative table, an illustration of the emerging concept of enterprise governance, benefits of good governance and a self-assessment questionnaire.

To recap a few key points, **figure 1** illustrates the distinction between corporate governance and enterprise governance. Enterprise governance refers to the comprehensive accountability framework that coordinates all management activity with respect to all stakeholders. Corporate governance primarily concerns the board of directors, the executive management team and the shareholders. External audit should report to the board. IT governance (not pictured) focuses on the use of technology to fulfill the organization's objectives as directed by management. Corporate and IT governance are two of the many components of enterprise governance. While corporate governance has garnered the media limelight most recently, it really is just one piece of the overall governance issue.


Figure 1

Stakeholders

Investors
Customers
Employees
Suppliers
Creditors
Community

Audit
Board
Executives
Enterprise Governance Corporate Governance

Strategic Planning and Alignment   Operations   Financials   Internal Controls

Source: Shamrock Technologies

Where the previous article focuses on the *differences* among the three disciplines, this article focuses on common elements. As illustrated in **figure 2**, there is overlap among the three

forms of governance. Although it is difficult to capture all of the nuances of governance, these common elements comprise some of the fundamental principles of good governance practice.

Figure 2

Enterprise Governance

Corporate Governance   IT Governance
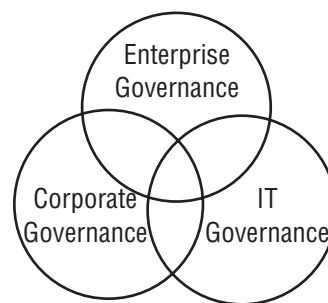
Definition, Clarification and Translation

Each form of governance contains the central themes of accountability, transparency, disclosure and independence. These qualities are needed to validate the integrity of the organization. But how are they to be operationalized? To answer this question, let's first get a better understanding of their meaning. Definitions for these key terms follow:

- Governance—The process of keeping under control
- Accountability—Answerable, capable of being explained
- Transparency—Easily understood, obvious, candid, open, can be seen as if there is no intervening material
- Disclosure—Bringing into the open, revealing
- Independent—Objective, no ties

Next, this understanding needs to be expanded. Since governance means the process of keeping under control, it would seem this implies that expectations either are known already or created proactively. Actions then are monitored, measured and corrected where necessary. In applying these terms collectively to the business world, one gets a feel for the essence of governance as redefined below:

- Governance means clear expectations are present.
- Transactions, decisions, business events and assets are handled responsibly. Recent events underscore the implication that records are accurate, reliable and auditable, i.e., can be explained, justified or supported in a manner that is understood clearly.
- Relevant information is disclosed in a timely manner.
- Where events deviate from expected tolerances, the events can be traced back and independently reviewed by an objec-

tive and reasonable audience that then can decide on corrective action or the next logical step to ensure that the organization improves over time.

- Further, there is an assumption that the organization proactively manages change.

Now, how are these qualities to be implemented? Perhaps more succinctly, what are the behaviors and characteristics common to all aspects of governance?

The authors believe that the tenets outlined translate into the best practices described below. These represent the key areas in which the board and executive team need to focus to build a well-governed enterprise.

Clear Expectations

Expectations might be more commonly referred to as organizational alignment or "getting everybody on the same page." Organizational alignment is best understood as an enterprisewide philosophy of consistent communication regarding values, strategies, initiatives, goals and objectives. Few surprises exist in organizations with a philosophy of keeping the entire organization focused and aligned. Organizational alignment is many things, but some of the primary components are:

Regardless of how the strategy is devised, it must be clearly communicated and apparent throughout the organization.

- Clear values—Organizations develop a value system/culture based on their actions and behaviors. If it is not guided by explicit design and clear policies, then it will develop implicitly by default. The tone needs to be set at the top in terms of mission, goals, attitude toward stakeholders, business tactics, internal controls, risk, ethics, sustainability and the degree of social conscience. These values permeate the enterprise and are evidenced in behaviors, attitudes, priorities, annual reports, public relations, ad campaigns and slogans, in the products and on the walls.
- Explicit policies and standards—Well-governed organizations maintain a clear and accessible repository of corporate policies, procedures and standards. These policies should be robust and current enough to provide reliable guidance. Policy documents cover the gamut of topics from dress codes, human resource policies, codes of conduct, acceptable PC use policies, as well as regulatory compliance policies. Having formal policies does not mean that everything is standardized; however, items that are critical to an organization's success should be standardized. Well-governed organizations reinforce the importance of these policies by making them part of employee orientation activities.
- Strong communication—Keeping organizations aligned and focused requires a philosophy and a culture of ample interaction. Not only do well-governed organizations exhibit excellent top-down communication, but they also value open and honest 360-degree communication that maximizes information flow to and from key stakeholders, including investors, shareholders, suppliers, customers, employees, whistleblowers and others. This is an open culture that addresses and vets concerns rather than disciplining those who communicate such concerns. In many complex organizations today, good communication includes establishing a standardized lexicon.

Even within the same country, terminology and part numbers can vary widely, especially when a company has grown by acquisition. In the high speed of today's economy, good communication implies a well-planned information access and delivery structure.

- Clear strategy—The strategic plan charts a course for the organization. There is a fair amount of variability across industries and within individual organizations as to how a strategic plan is developed. The degree of active involvement by the board of directors, in particular, varies considerably. In most companies, the strategic plan is developed by the senior management team under the auspices of the board of directors. Collectively, senior management oversees the strategic planning process, sets the strategic plan and approves a corresponding budget. In some organizations led by a dominant CEO and/or chairman of the board, the strategic plan is a dictate of his/her vision, approved by the board. In some organizations, the board of directors essentially sets the course and the senior management team acts in a stewardship role for its implementation. Regardless of how the strategy is devised, it must be clearly communicated and apparent throughout the organization. At well-governed organizations, the executive team considers and includes all reasonably relevant perspectives and the related trade-offs by soliciting input from a variety of sources, including customers, staff, suppliers and other stakeholders. Resource allocations of people and capital are assessed against short-term goals as well as longer-term objectives. The balanced scorecard[3] is a popular tool designed to help align and prioritize objectives. Participation helps all parties to get buy-in on the final priorities and then strive together to fulfill them. Coordination helps minimize overlaps, redundancies and projects at cross-purposes. Strategic plans are reviewed and updated periodically in light of the changing business environment.

Handled Responsibly and Clearly

Transactions, decisions, business events and assets are handled responsibly. Recent events underscore the implication that records are accurate, reliable and auditable, that is, can be explained, justified or supported in a manner that is easily understood. This presumes that sufficient resources are provided to support the following components:

- Competent organization—A strong staff is needed to carry out the mission of the enterprise. Roles and responsibilities are documented clearly. Employees need constant education, especially on company policies, procedures, internal controls, safety and orientation to reference documents (on the web or in the organization). Terrorism has brought renewed attention to safety issues resulting in increased background checks, access authorizations and third-party vendor reviews. The organizational structures must adapt constantly to changing business demands. Well-governed organizations not only adjust staff to match demand reflected by variations in economic conditions, but they periodically adjust skills and expertise.

- Orderly processes—Process documentation and management have become increasingly critical with the growth and complexity of today's environment. Every business process MUST be owned and managed by a business unit. If the process is identified as critical, it must be assigned a business owner (even if it is automated). With ownership comes the responsibility for the process to be logically designed, clear, robust, documented and auditable. Risk should be assessed and managed accordingly with the appropriate application of internal controls. All key records, business files and data are created accurately and reliably, cataloged effectively, secured when sensitive from unauthorized access and disposed of properly. Business continuity plans should be created, communicated and tested for operations as well as information systems.
- Effective IT—Well-governed organizations typically have a "relatively" cohesive IT infrastructure that supports and enables the business. IT is treated as a critical asset that must be managed effectively. Information support systems are implemented in a manner that strives to ensure that the system best fits the needs and is compatible with the organization's infrastructure, reasonably priced, responsibly tested, installed, adequately documented and well maintained. For many of today's organizations IT is the key asset by which the organization functions. The IT environment is the vehicle by which metrics are collected, the mechanism responsible for automating many control functions, and the underlying structure used to enable organizationwide communication. For some, it is the key enabling vehicle for process improvement
- Responsible asset management—Keeping track of company assets is not a new proposition. Historically, asset tracking has focused on facility and financial asset management. Well-governed organizations institutionalize asset management. Processes and procedures are well entrenched to identify, track and oversee the organization's assets. Leading organizations have expanded their definition/classification of assets beyond the traditional physical and financial assets to include IT components (including laptops and PC software licenses) as well as intellectual capital, legacy knowledge, business processes and other information assets.

Timely Disclosure

Relevant information is disclosed in a timely manner. The measurement of formal performance metrics is an extension of the principles of clear strategy, strong communication, independent review and continuous improvement.

Well-governed companies know the value of the phrase "what gets measured gets managed." Performance measures are used to reinforce and align organizational behavior. In nearly every well-managed company, performance metrics are used as a key underpinning of variable compensation for all levels of the organization.

Strategically and organizationally aligned companies have clear and consistent performance measures. Performance metrics are linked directly to all, or some combination of, key

operational metrics and key market metrics, and they measure the progress toward strategic goals. These performance measures are standardized, objective and supported by well-designed, documented and auditable processes and reports that succinctly provide a wealth of key indicators, alerts and trends.

Many organizations today have automated most of the collection and reporting of performance measures. Some of these systems now are expected to provide near real-time public reporting of significant events. Management needs to ensure that these systems are well designed, tested and auditable. A particularly vulnerable area is where multiple systems have been interfaced or rolled up due to organizational restructurings.

Independent Review and Continuous Improvement

Where events deviate from expectations, they can be traced back and independently reviewed by an objective and reasonable audience that then can decide either on corrective action or the next logical step. There is an implicit assumption that the organization improves over time, and this criterion is fulfilled by internal controls.

The landmark study, *Internal Control-Integrated Framework*,[4] is regarded as having established the first widely accepted industry standards for internal control. More commonly referred to as the "COSO study," it was published in 1992. It defines internal control as: "…a process effected by an entity's board of directors, management and other personnel, designed to provide management reasonable assurance regarding the achievement of objectives in the following categories:
- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations"

Internal controls, in this discussion, are broadly used and include audit, risk management, loss prevention, quality assurance and continuous improvement. Trust is at the core of commerce and is essential for long-term success. Together these disciplines provide a process that allows for the systematic review of risk, threats, hazards and concerns, and then provides cost-effective measures to lower the risk to a reasonable level as well as continuously improve operations.

Proactive Change Management

To survive, organizations must adapt to the changing environment. Well-governed organizations are proactive in this regard, in an effort to shape their own destinies. With increased complexity comes the need for executives to recognize and obtain the additional resources and management time needed to stay ahead of the chaos curve. Typical change management issues are:
- Special circumstances—In addition to ordinary business, international, societal and technology trends, there are many special circumstances that significantly increase the complexity of managing an organization. A few examples are:
    – Mergers, acquisitions, divestitures, IPO, deregulation—As companies add, change or shed operating

> *Well-governed companies know the value of the phrase "what gets measured gets managed."*

units, there is a corresponding need to absorb or disengage processes, staff, infrastructure, marketing materials and so forth.

- Third-party vendors—Where there is a heavy reliance on external business partners, there is an increased responsibility to manage those relationships.
- Multiple locations—When organizations expand to multiple locations, there is increased complexity in determining which operations need to be standardized for economy and security, and which operations have a legitimate business need to remain unique. These locations can be data centers, distribution facilities, regional offices or manufacturing plants.
- Global business considerations—Going international can expand the complexity of operations exponentially. In
addition to the all issues listed above, there can be issues of language, time zone, technology infrastructures, government regulations and cultural adjustments.
- Major projects—Depending on the volume of major initiatives, there may be temporary or permanent resources dedicated. One common example is a project management office. This group may apply to a special business initiative; however, it is commonly seen for technology projects. Permanent project management offices supporting multiple initiatives can support business sponsors in the design of investment programs and the preparation of value cases.

• Governance coordination—Governance is an example of an emerging change management need. The governance components described in this article may be called by other names, looked at in a different order, or addressed in an infinite number of ways by organizations; however, executives must ensure that these critical components are addressed. In most companies, existing governance efforts are spread across a number of business units—finance, legal, IT, human resources, risk management, corporate secretary and others. Governance components do not necessarily fall into existing slots on the organization chart. Recognizing them and designating a person to take the lead are the first challenges of change management. A plan must be developed, often with little guidance. Like many other change management initiatives, it may take an interdepartmental approach to address it properly.

Governance Breakdowns

The previous discussion on the basic elements of governance may seem basic; however, the rapid expansion in the 1990s, followed by the searing economic downturn of recent years, and punctuated by mergers, acquisitions, reorganizations, bankruptcies and downsizings, has created a superstructure at many companies that is hazy and often inefficient and costly. In the more severe cases, it is chaotic or open to devastating liability.

The cost of slack governance does not appear on expense budgets, it appears in the media, in share prices, in the waste bin or behind closed doors. In governance breakdowns, operational problems make executives *appear* incompetent. Examples include the following (note that these problems do not stem from financial statements *per se*, and may not necessarily be from criminal executives):

• Question of integrity—For example, Boy Scouts are universally regarded for their honesty, integrity and tracking skills. Located just minutes from Boy Scout headquarters, the fifth largest of 324 franchises, Circle Ten in Dallas, Texas, USA, is under federal investigation looking into allegations that it inflated its roster of minorities by as much as 30 percent to boost charitable donations and justify higher financing requests by including long-expired "ghost troops," or members who had grown up and had children of their own, and members shown to live at an apartment complex that was bulldozed years earlier. The organization purged 25 percent of its membership rolls after the federal investigation by the US Postal Inspection Service began. Circle Ten officials complain that their credibility remains at issue until the matter is resolved.[5]

• Due process—Dallas (Texas, USA) County Sheriff Jim Bowles has been criticized for awarding a US $20 million bid to a longtime business friend who *appeared* to provide significantly less revenue to the county jail than competing bids. A ruling by the state's attorney general forced the sheriff to release the bid documents for public review. Protests from competing vendors called into question the county's award process, criteria for selection and the impartiality of the evaluation. Although there has not yet been any evidence of illegal activity, the competency and reputation of the sheriff, the county and government in general have been tarnished.[6]

• Loss of US $5 billion—The US Agriculture Department lost track of US $5 billion in taxpayer funds, and investigators could not tell whether the missing cash was a result of theft or sloppy bookkeeping, according to the agency's inspector general. The department requested the US Congress give it US $100 million to locate the missing revenue. "The bottom line is that we do not know" where the money is, Inspector General Roger Viadero stated at a hearing in front of the US Congress.[7]

• Mismanagement is priceless at the Louvre—Mismanagement causes loss of artwork, computer equipment and staff time. "French auditors....delivered a damning indictment of management at Paris' best-known museum, the Louvre, where staff work one day for two paid...The French government has also been concerned about large numbers of thefts, not just of artwork but of computing equipment and audiovisual aids in particular, most apparently committed by staff. The inventory is so poor, it is difficult to even estimate the loss...The court report said another financial anomaly meant the Louvre was deeply short of cash for maintenance work and staff."[8]

• Operating inconsistencies across entire organization—Begun in 1997, Nestle USA spent US $210 million and six years on an ERP implementation project that was halted in mid-rollout because the implementation was fraught with dead ends and costly mistakes. The team found, among many other troubling redundancies, that Nestle USA's brands were paying 29 different prices for vanilla—to the same vendor. Each division and every factory called the item by a different item

number, and as a result, there was no way to compare. "I don't think they knew how ugly it was," says Jeri Dunn, CIO of Nestle USA. "We had nine different general ledgers and 28 points of customer entry, and multiple purchasing systems."[9]

- ID theft—Credit information for some 30,000 people was stolen in a scheme where a help desk worker at Teledata Communications sold passwords and codes for downloading consumer credit reports to an unidentified person. Teledata, a software company, provides banks with computerized access to credit information databases. More than 15,000 credit reports were stolen from Experian, a credit history bureau, using passwords belonging to Ford Motor Credit Corp. Thousands of other credit reports were stolen from other companies. According to the US Justice Department, there are 500,000 to 700,000 cases of identity theft in the US each year.[10]

Governance Successes

The following stock exchanges and fund indices have been set up exclusively for companies that have a strong emphasis on good governance practices. Each of them has outperformed comparable indices. It appears that good corporate governance practices provide value for long-term sustainability as well as shorter-term results.

- **STAR Exchange**—Italian stock exchange for small to mid-size companies that follow strict governance requirements. These 37 companies with a total market capitalization of US $7.5 billion outperformed counterparts on the Borsa by 16.5 percent between April 2001 and March 2002.[11]
- **Novo Mercado**—An exchange similar to STAR opened in Brazil.
- **Stock Exchange of Thailand**—A study of the 100 largest companies found that clearly the companies with strong corporate governance have higher market valuations. Investors pay a premium, especially for companies that adopt international best practice standards.[12]
- **Dow Jones Sustainability Index (DJSI)**—Has outperformed the Dow Jones General Index (DJGI) from 1996 through 2000 (the latest date of the study).[13]
- **Deutsche Bank**—Study shows that companies with good governance outperformed peers on the SA Morgan Stanley Capital Index (MSCI) in earnings and share prices by 52 percent and 72 percent respectively over one, three and five years. In Latin America, premiums paid average 23 percent on price to earnings; in South African it is 59 percent.[14]

Governance Reform

There is no question that there has been, and will continue to be, growing attention to executive accountability and governance issues around the globe, particularly for publicly held companies. In response to the rash of US corporate malfeasance in 2002, there has been a maelstrom of calls for *corporate governance* reform. The US Congress rapidly passed the Sarbanes-Oxley Act of 2002, which sharply strengthened many requirements for independence, ethics and internal controls. It significantly stiffened the penalties for fraud as well as for

CEOs and CFOs who knowingly certify information that is known to have material deficiencies or omissions.

At the same time, various international stock exchanges and watchdog groups are proposing and evaluating their own requirements for improved *corporate governance*. Hence, around the world, corporate boards already are reviewing their practices to address such issues as executive compensation, board independence, stock options, codes of ethics, audit committees and rotation of external auditors. Note that many of these issues could be resolved by a company within a matter of months given a concerted effort.

The US Sarbanes-Oxley Act is now in various stages of clarification and implementation. Many experts believe that the US Securities and Exchange Commission should take this opportunity to send a strong message to corporate executives by specifying a much broader definition of internal controls than that in the past which focused strictly on financial statements and regulatory compliance. Specifically, most industry experts (at this writing) are recommending that the COSO definition of internal controls[15] be referenced and used as a standard for Section 404 "Management Assessment of Internal Controls" and procedures for financial reporting. The COSO definition extends the concept of internal controls to include "effectiveness and efficiency of operations" that support the financial reporting process. Under this definition, areas that may have material impact on the organization or its financial reporting preparation process would need to be included in the assertion by senior management. This would include such additional areas as information processing and environmental issues. The COSO definition would help to address some of the fundamental principles of governance raised in this article.

Conclusion

The underlying principles and characteristics represented in well-governed companies are not new. However, governance integrates all of these aspects across the organization in a cohesive manner that better reflects the intentions of management. What is clear from today's headlines is the need for top executives to take a second look at governance in light of increased market, shareholder, political and regulatory sensitivity. In many cases, they are likely to find renewed justification to step up the level of attention to their governance processes.

Today's executives need to create a governance infrastructure that institutionalizes a strong accountability framework. The key to governance is to orchestrate all efforts in a manner that maximizes value. The degree to which top management can focus the organization, institutionalize its mandates and optimize its use of resources will go a long way toward determining the success of the organization.

The media spotlight is now on corporate governance; however, as owners, boards and executives look toward the specific aspect of assessing their internal controls, they will realize that stronger fundamental governance practices will strengthen their overall accountability, transparency and disclosure capabilities.

It is hoped that this article has taken the abstract concept of governance and translated it into actionable items that firms can use to strengthen their own governance practices. The best

place to start is by designating someone to coordinate these efforts, perform a current governance assessment and develop a plan that balances the values and the resources of the organization.

Endnotes

[1] Hamaker, Stacey; "Spotlight on Governance," *Information Systems Control Journal*, volume 1, 2003

[2] *The American Heritage Dictionary of the English Language*, American Heritage Publishing Co. Inc., New York, USA, 1973

[3] Kaplan, Robert S.; David P. Norton; *The Balanced Scorecard*, Harvard Business School Press, Boston, 1996

[4] Warren, Edelson, Parker, and Thrun; *Handbook of IT Auditing*, Coopers & Lybrand LLP, Warren, Gorham & Lamont—RIA Group, New York, USA, 1998

[5] Bensman, Todd; "Boy Scout roster inflation getting grand jury scrutiny," *Dallas Morning News*, 5 January 2003

[6] Housewright, Ed; "AG's ruling prompts sheriff to release bids," *Dallas Morning News*, 14 September 2002

[7] Scripps Howard News Service, "Agriculture Department says it's missing $5 billion," *The Dallas Morning News*, 29 September 2000, pg 4A

[8] "French Auditors Paint a Picture of Failure at Louvre," *The Toqueville Connection*, 1 February 2002, *www.ttc.org/cgi-binloc*

[9] Worthen, Ben; "Nestle's ERP Odyssey," *CIO Magazine*, 15 May 2002, *www.cio.com/archive/051502/ nestle_content.html*

[10] "Feds hunt ID Thieves," CBSnews.com, New York, USA, 26 November 2002, *www.cbsnews.com/stories/2002/ 11/13/tech/printable529217.s html*

[11] Hoschka, Tobias C.; "A market for the well governed," *The McKinsey Quarterly*, 2002, Number 3

[12] "Better Boards in Thailand," *The McKinsey Quarterly*, 5 September 2002

[13] *www.kodak.com/US/en/c...t/01CorpEnviroRpt/ practices_sustain.jhtml*

[14] "Study Shows it Pays to be Virtuous," *Business Day* (South Africa), 23 October 2002

[15] *www.coso.org*

Stacey Hamaker, CISA
is managing principal of Shamrock Technologies, which provides strategic, enterprisewide analyses, requirements definition, project management and internal control services to public and private sector clients. A published author on governance issues, she has 25 years of experience with enterprisewide technology initiatives at *Fortune 500* and midsize clients.

Austin Hutton
is principal at Shamrock Technologies and is a demonstrated leader with experience managing global technology organizations for *Fortune* 50 companies. He serves as a contract CIO and develops and manages consulting practices.