Vasant Raval, DBA, CISA, ACMA, is a professor of accountancy at Creighton University (Omaha, Nebraska, USA). The coauthor of two books on information systems and security, his areas of teaching and research interest include information security and corporate governance. Opinions expressed in this column are his own and not those of Creighton University. He can be reached at *vraval@creighton.edu.*

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca. org/journal)*, find the article and choose the Comments tab to share your thoughts.

Go directly to the article:

Monitoring Morality
Is Assurance of Information Ethics Feasible?

My honest thought about monitoring is: I do not like being monitored! I am not alone. A large majority of individuals and organizations would assert that they do not like being monitored. And yet, it has benefits, such as the potential for corrective action, behavior modification and improvement in performance. Monitoring, including self-monitoring, helps gain and maintain others' trust as well. If monitoring can be digested as a palatable thought, the next question is: Can we—should we—monitor morality in organizations?

Why monitor morality? As John Rosthorn said, "The more serious survival issue for top managers and investors is not competition, but the enemies within the corporation."[1] The "enemy within" has to do with actions of someone (or a group of people) influential in the enterprise breaching the trust of its stakeholders. Organizations—whether for-profit or otherwise—thrive on their stakeholders' trust in them. All legitimate organizations need to protect and manage this trust in order to guarantee their continued viability and prosperity. People both within and outside the enterprise have expectations and trust that the organization will deliver on its promises. Any cracks in this trust, often a consequence of poor risk management, result in a crisis of confidence in the organization. Consequently, a perfectly running organization may face extinction if the trust gap widens. As an example, consider the recent introduction of a new generic top-level domain (gTLD) name, *.sucks*, by Icann, the traffic cop of the Internet. Icann's approval of the .sucks domain rested on hearing no objections from anyone, hardly a responsible justification, given the global influence Icann holds.[2] This has engendered a crisis of confidence in Icann, for the new domain could prove to be predatory, exploitative or coercive. Consequently, subscribers, regulators and erstwhile users of the global network wonder if Icann will maintain its historic path of integrity and objectivity.

So there is a need for the enterprise to nurture and maintain trust, which, in turn, depends on how well it fulfills its duties rather than how aggressively it chases its rights. The normative ideas of trust and duty need to be put into practice to observe and assess an organization's behavior within the context of ethics. For this, we must recognize two related dimensions:
1. Stakeholders of the organization
2. The organization's performance

STAKEHOLDERS
Any entity that involves people will have to face separate concerns for each of its stakeholders (e.g., investors, employees, the community) in addition to dealing with its overarching need to harmonize these into a broader set of values embedded in a common vision and a code of ethics. The diversity of stakeholder groups' needs should be built into and coordinated within the overall ethical climate of the organization. An IT training school, for example, should offer its students information security skills that their prospective employers can use, while at the same time striving to ensure that it does not graduate "raw" hackers with little or no ethical sensitivity.

Finally, whereas duty toward each stakeholder must be addressed, it is equally important that a balance be achieved among all of the duties toward a stakeholder group and between the expectations of various competing stakeholder groups. For example, passenger safety concerns of a railroad should not be relegated only to buying casualty insurance, and the decision on energy use should not disregard environmental issues while minimizing train operating costs.

PERFORMANCE
Trust of stakeholders is sourced in three key categories of influence and accountability of a business: economic, social and environmental.[3] Of the three, the concept of economic accountability has been developed well over the past several centuries. There are metrics in

place, such as the general-purpose financial statements that provide insights into the financial health of the business. Also, regulatory requirements have attempted to enforce the need for trustworthy information. This, in turn, permits the business's stakeholders to assess how well the company has delivered on its promise to generate a return on investment (ROI) in the company. The accountability and reporting issues in social and environmental categories are being more aggressively examined recently, although there is still a great deal of room for further development and maturation. One idea is to develop an integrated, multidimensional reporting of enterprise performance, called the "triple bottom line" (3BL), an accountability framework with three parts—social, environmental and financial—often considered the three pillars of sustainability. Besides each dimension representing a separate domain, it is equally important to recognize trade-offs across the three dimensions. For example, financial results of a particular period or periods may be improved by marginalizing environmental objectives or killing the community involvement of the organization.

The idea of trust across these performance categories accompanies the stakeholders' concern as to how well the organization will measure up to it. After all, an entity's actions could run counter to its promises and expected behavior. Because businesses are agents of their principals, such as the shareholders, there is a need for assurance that the results reported are audited by an independent, competent professional with integrity and objectivity. Whether a single bottom line or triple bottom line, key performance reports to stakeholders deserve an endorsement of assurance by an independent party.

Any attempt to assess organizational performance should examine all intersecting cells, between stakeholder groups on one side of the table and the three dimensions of performance—financial, social and environmental—on the other. To illustrate, take the example of privacy as an issue. Privacy issues can be represented as a subcategory of the social dimension of Google. Because Google has vast influence on privacy of user data, it has been asked by the US Federal Trade Commission (FTC)—as have others—to have a privacy audit conducted. In this case, the stakeholder group is the user (including, perhaps, the regulator) and the category of the organizational dimension is the social aspect. Depending on the nature of the organization, its business

model and its strategy, intersecting cells would likely vary in terms of criticality and relevance. Privacy issues, for example, may not be as critical to a home builder as they would be to a business such as LinkedIn.

ETHICS AUDIT

The term "ethics audit" or, preferably, the "assurance of ethics" is not widely used in literature and is sometimes confused with ethical auditing. In essence, an ethics audit is a systematic review of the expressed or implicit ethical obligations of an enterprise to assess how well this portfolio of moral obligations was met by the leadership of the enterprise during the period of time examined. The following propositions seem to articulate well the idea of assurance of ethics:[4]

- An organization is, at its core, a social institution.
- The organization conducts itself within the bounds of a set of basic values.
- Management's actions and behavior are essential expressions of these values over time.

To illustrate, Amtrak (USA) endows an important social dimension as it serves millions of passengers. One of its values has to do with passenger safety. A recent northbound train near Philadelphia, Pennsylvania, USA, was speeding at over 100 miles per hour, more than twice the speed limit, and became derailed. Several lives were lost and many passengers were injured. The automatic train control (ATC) technology currently in place is limited in comparison to the more sophisticated positive train control (PTC) technology, and the use of ATC has been put forth as a key reason for the tragedy. Presumably, the true reasons may be evident in the allocation of resources toward this duty; deferment of decisions to address high levels of risk in certain track areas; poor employee training; or the lack of awareness of or low sensitivity to passenger safety as an organizational objective. Only an in-depth investigation of the incident will reveal the exact nature of causes leading to the disaster.

LEADERSHIP

Across the three dimensions—economic, social and environmental—of a business, one thing that is common is leadership. The top leaders craft the internal environment and nurture and support the overall accountability of the entity to its stakeholders. Management's commitment to the

written word of conduct is crucial to the ethical expression in everything that management decides and every way it leads the organization.[5] Trustworthy behavior has the underlying element of risk management; that is, how well does the company manage the risk of doing business in a morally responsible way?

If we were to look for one indicator of moral threads that bind leadership in a business, it would probably be the tone at the top. The external auditors consider it important to review the client company's tone at the top as an overarching fraud risk factor.[6] If the tone is poor, chances are leadership behavior may fall short in its resolve to do the right thing. Take the case of Tianjin University in China. Six individuals, including three professors from China, while on sabbatical at a US university, allegedly swiped secrets from US companies relating to how to filter out unwanted signals in wireless devices. Upon their return to China, Tianjin University collaborated with the professors to form a start-up to produce and sell equipment using the technology.[7] The bottom line: Tianjin University appears to have failed to uphold its integrity.

In contrast, continuing the example of transportation safety, look at the case of the Union Pacific Corporation (UP). UP is mostly in the business of moving freight. However, it places utmost importance on the safety of its people, customers and communities at large. The company lives by its promise to protect people from potential harm as it drives its economic agenda. And UP makes resource allocations to ensure that safer, more current and sophisticated PTC technologies are in place to ensure safety: a key moral commitment of the corporation.

IS ASSURANCE OF INFORMATION ETHICS FEASIBLE?

I am quite optimistic about the prospects of assurance of information ethics. Yes, there is a great deal of work that needs to be done to develop models and paradigms that will permit a clear articulation of the *how* portion of the assurance process. Perhaps the three broad propositions noted in this column will provide a basis for further analysis and design.

How does an assurance of ethics differ from an assurance of information ethics? The two certainly seem to overlap a great deal. However, the emphasis in the assurance of information ethics should be on information objectives, technologies, platforms and processes, and outputs—all examined from the perspective of ethical conduct by the organization. One possibility is to extend COBIT® 5 to a specific and clear mapping of information ethics.

As is becoming well known, ethical dilemmas from fast-paced innovation in the IT-enabled environment are emerging and will have to be addressed. For example, Amazon, among others, will have to find ethically responsible ways to deploy drones, and Google will have to continue to wrestle with privacy issues while working on global and fair access to information. Mobile devices and the Internet of Things (IoT) will make life exciting, but even before harnessing the good, abuses of technology could overwhelm the IT professional. In this increasingly complex environment, a disciplined approach to account for information ethics should prove worthwhile.

ENDNOTES

[1] Rosthorn, John; "Business Ethics Auditing—More Than a Stakeholder's Toy," *Journal of Business Ethics*, 27: 9-19, 2000, p. 9

[2] Elder, Jeff; "A Debate Over the Domain '.sucks,'" Digits: Tech News & Analysis From the WSJ, 29 May 2015, *http://blogs.wsj.com/digits/2015/05/19/new-domain-sparks-icann-debate/*

[3] Garcia-Marza, D.; "Trust and Dialogue: Theoretical Approaches to Ethics Auditing," *Journal of Business Ethics*, 57: 209-219, 2005

[4] *Op cit*, Garcia-Marza, p. 215

[5] For example, the recent disclosures of the alleged bribery scandals at the Federation of International Football Associations (FIFA) suggest a weak tone at the top, despite elaborate documentation of enforcement requirements of ethical practices of the sport.

[6] See, for example, Apostolou, B. A.; J. H. Hassell; S. A. Weber; G. E. Sumners; "The Relative Importance of Fraud Risk Factors," *Behavioral Research in Accounting*, 13: 1-24, 2001.

[7] *The Wall Street Journal*, "U.S. Says Chinese Professors Stole Tech," 20 May 2015, p. A1