Seven Myths of Information Governance

The term “governance” has different interpretations depending on the perspective of the user. In mechanical engineering, the term “governor” conveys the presence of a feedback device on a machine (system) that is used to provide automatic control of, for example, speed, pressure or temperature. As defined by ISACA, governance ensures that “stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives.”

In essence, the role of governance is to empower the principal to monitor and control the behavior of the agent. For example, in corporate governance, the principal—particularly the shareholder—is represented by the board of directors, which is charged with the duty of oversight over management. The purpose of corporate governance is to persuade, induce, compel and otherwise motivate corporate managers to keep the promises they make to investors. In addition to these high-level meanings assigned to governance, the notion of governance can also be discussed from the viewpoint of firm characteristics (e.g., public vs. private companies, large vs. small companies, partnerships), sector (e.g., hospitals, government, cooperatives, nonprofit entities) or stakeholder orientation (e.g., shareholders, customers, employees, the public).

Interestingly, governance is also used to convey the monitoring and control of different intraorganizational domains of an entity. When used in this sense, governance suggests a subset of entity-level governance. For example, the overall governance of an entity encompasses information governance—monitoring and control of data capture, data storage and creation, and distribution and use of information. Information governance, in turn, includes data governance. When a major technological innovation becomes a key driver of the economy, the innovation could take on its own governance angle, e.g., governance of cloud computing. Thus, the variety and shades of governance perspectives could be confusing and counterproductive if, at the outset, it is not clear which part of the governance schema is the reference point for the discussion. In this article, the term “governance” is used in the sense of information governance to discuss certain myths or misunderstandings of governance.

FOCUSES OF GOVERNANCE: RESOURCES AND PROCESSES AND BUSINESS VALUE

The Committee of Sponsoring Organizations of the Treadway Commission defines “enterprise risk management” (ERM) as follows:

Enterprise risk management is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

The notion of governance entails the monitoring of ERM, which is strategic in nature, is driven by processes and aims at the achievement of intended objectives. Thus, governance involves guiding and steering the process so that the process remains in control and continues to deliver desired results in terms of business value (BV). A process “remaining in control” and “delivering desired results” are two related, but distinct, focuses of governance.

The resources and processes focus refers to controlling risk of processes and resources; the BV focus involves monitoring decisions to create BV. Although notionally separate, the two focuses influence each other because every initiative to deliver BV is likely to be accompanied by additional risk that may warrant additional controls. For example, a business acquisition...
possibly adds BV while also adding to the need to control the
resources and processes of the larger entity.

In the arena of information governance, the resources and processes focus suggests the need to control information resources and processes to mitigate their risk exposures and achieve systems performance goals. This focus ensures that IT resources and processes and their performance and risk management are addressed. Often, this is achieved through cost budgets. Concurrently, the BV focus centers on control of the system behavior so that expected information outcomes are delivered to the users. The resources and processes focus centers on processes that create information, and the BV focus centers on processes that use information to generate BV.

The accountability for IT resources and processes is easier to identify and evaluate than the accountability for the creation of BV. BV emerges throughout the organization, and while IT may be a facilitator in doing so, it may not be the sole or dominant actor. BV from IT investments cannot be realized by IT, but will always be created on the business side, sometimes using technology as a co-creator of BV. The BV focus has to do with the actor, as distinguished from the creator of information, who uses information for value creation by providing other goods and services and by making and supporting decisions, which, in turn, may generate further information or intelligence.

With the resources and processes focus, systematic development, implementation, maintenance and monitoring of controls help mitigate risk to systems and processes that deliver information. On the other hand, the BV focus impacts the organization’s value performance, often determined in financial terms. These outputs (e.g., as summarized in financial reports) also need to be measured, monitored and disclosed appropriately. Thus, information resource management is primarily driven by the resources and processes focus of creators, and delivering BV is primarily driven by the BV focus of actors.

Because the accountability of a creator of information is different in nature (e.g., cost control emphasis) than the accountability of the actor (e.g., cost savings, additional profits, return on investment), it is often convenient to separate the discussion of resources and processes to generate information from those that add BV. External auditors, for example, provide their opinion on the control framework (resources and processes focus) of their auditee, which is then followed by an opinion on the financial statements (BV focus).

The two focuses overlap and impact one another. Take, for example, a decision to outsource some IT services to a cloud computing environment. This decision may result in cost reduction, which, in turn, improves operating profits—a measure of BV. However, the decision also leads to new risk that needs to be assessed and mitigated. The decision also impacts the risk of resources and processes that create information. Although the underlying decision involves both focuses, knowing the difference between the roles of the two and providing requisite variety to control each are critical in effectively addressing information governance issues.

Use of the term “information governance” in a broad sense often leaves out or implicitly assumes the focal point. Is the focus on controlling resources and processes that create information, or is it on those resources and processes that use information outputs to create BV? Although the treatment of each focus is best done in somewhat separate ways, there has to be clarity on the two focuses of governance, how each is achieved and where the two converge. Within this context, this article discusses certain misconceptions of information governance; illustrates key points; and, where possible, suggests ways to overcome such misconceptions. Of these, the first four myths presented clearly point to a weak distinction between the two focuses of information governance—resources and processes, and BV.

**MYTH 1: RISK IS SEPARATE FROM OPPORTUNITIES**

Every move on the part of an organization comes with risk and opportunities, and both must be managed. While there is temptation to leverage an opportunity, it should not be entertained without regard to the landscape of risk that the business decision will change. Thus, risk is not separate from opportunities, and considering one and leaving out the other is not an option. Where a firm’s emphasis is in favor of opportunity and against risk, the positioning of the chief risk officer (CRO) is ineffective because risk management is not valued as an equal discipline to opportunity pursuit.

Often, problems arise from thinking that the governance of risk related to resources and processes is unrelated to the
The governance of BV (BV focus). Decisions about risk management are in tandem with decisions about exploiting opportunities to improve substantive performance. Addressing risk, for example, from outsourcing to cloud services may be seen as a process evaluation, whereas exploiting the opportunity may be gauged in terms of the present value of cost savings from outsourcing. In terms of accountability, risk could fall in one area (e.g., the chief information officer) and financial performance management in another (e.g., the chief financial officer). Thus, the burden of taking on a new opportunity could fall exclusively in one area and potential benefits may be credited to another. While there may be a general understanding that risk and rewards come together, in reality, accountability for each may be segregated and may never get reconciled on the same page.

The frameworks that provide structure to information governance are COBIT and Val IT. Roughly, COBIT leans toward the resources and processes focus and Val IT leans toward the BV focus. Whereas each framework supports the unique needs of each governance perspective, there must be an effective, sustained alignment between the two. Several measures can be taken to meet this end. For example, business key performance indicators (KPIs) can be mapped to IT KPIs and an appropriate set of balanced scorecards (BSCs) can be developed to link business and IT KPIs. Whereas these steps will likely help, a systematic development of a comprehensive "bridge" between COBIT 4.1 and Val IT can provide the greatest benefit, as seen in COBIT 5. Such a bridge can offer a common ground to both creators and actors of information in which the accountability for alignment is shared by both groups.

**MYTH 2: GOVERNANCE IS A DESTINATION**

As discussed previously, governance warrants monitoring the risk and opportunity sides of every event, current or proposed, in light of the intended objectives. It is not a one-time event; it is a journey. Related to the resources and processes focus, continual evaluation of the control framework and, where necessary, appropriate corrective actions may not occur, leaving new areas of risk unmitigated and keeping in force controls that address risk that no longer matters to the organization. On the BV focus, continual innovation in business strategy and value creation is imperative; it is also not a one-time event.

In part, this sort of impression—that governance is a destination—could result from the perception that controls, once designed, continue to effectively serve the risk mitigation objective and, therefore, the only thing that needs to be cared for on an ongoing basis is the creation of BV, not mitigation of risk. It is likely that those in charge of information governance are not convinced that continual evaluation and realignment of the control framework that serves the resources and processes focus can be cost-effective. Once the framework is in place, they may see comfort in what already exists. If so, it would be necessary to discourage the mindset that what exists does not require a second look, especially when the company makes major operational, tactical or strategic changes on the business side to impact future outcomes. For example, if a company decides to lay off several hundred employees, it will likely improve the bottom-line financial performance; however, this will also raise questions of potential gaps in process controls created by the departure of people in key positions.

In fact, compliance initiatives never really end. To ensure continuous compliance, a model such as Deming’s Plan-Do-Check-Act cycle should work well.

**MYTH 3: REGULATORY COMPLIANCE IS THE KEY OUTCOME**

Regulations and laws have a place in society and business. Without legal requirements, it is difficult to ensure that a company does all that is necessary. Consequently, much credit is given to the US Sarbanes-Oxley Act and Europe’s Basel II for requiring corporations to meet threshold governance requirements.

Thus, regulatory compliance with enacted governance standards has become an overwhelming force. Just recently, some members of the US Congress have encouraged the US Securities and Exchange Commission (SEC) to require companies to disclose incidences of data breaches and related facts about their information systems. Additional burdens of monitoring and disclosure requirements could cause the governing authorities, such as the board of directors, to feel that meeting the letter of the law is sufficient. “An often-mentioned myth or misunderstanding is that better governance...will take too much time or cost too much. This is typically mentioned by people who think that ‘governance’...
means only dead-weight compliance.”15 The perception that may further reinforce this behavior is that there are no tangible benefits, just costs, of doing more. Consequently, organizations may not subscribe to additional governance measures as value-added initiatives.

However, first and foremost, governance is supposed to benefit the owner entity. Hence, to stop at the door of compliance and do nothing more with it is a disappointing state. For example, the SEC has recently mandated that public companies must use Extensible Markup Language (XML)-based Extensible Business Reporting Language (XBRL) tags to meet the agency’s filing requirements. Companies can do this in two ways: by “bolting on” the tags to the final filing papers or by embedding the tags throughout the general ledger of the company. The latter option potentially benefits the company in that the tagged data could be used by management for efficient and effective decision making. Often, instead of considering this avenue in which lasting benefits could occur to the company, most filers are likely to use the shortcut of bolting on the tags. The result is that the benefit of using the tags to track transactions (e.g., to prepare internal reports to compare plans with actual performance) is not chosen; only the regulatory compliance requirement is met.

Regulations related to risk management and related disclosures set the minimum across-the-board generalized requirements. Where good governance exists, meeting legal requirements is likely to be the least concern. If anything, compliance in such cases would have an ancillary effect rather than a primary outcome.

Finally, regulatory compliance, by itself, may project only the resources and processes focus, which is not enough to execute the company’s business strategy. The BV focus is an integral aspect of information governance.

To address this myth, business and IT leaders should emphasize a customized approach to meeting these requirements within their firms, producing synergy well beyond the regulatory threshold. This is why tone at the top—including consistency among statements, assertions, and explanations of management and its actions—is vital to effective governance.16

**MYTH 4: GOVERNANCE IS SEPARATE FROM BUSINESS PERFORMANCE**

This myth is a corollary to the first myth. From within an organization, one may look predominantly from the viewpoint of mitigating risk related to resources and processes. However, the delivery of BV through management’s actions, the BV focus, is also integral part of governance. Is it likely that management places a disproportionate weight on the resources and processes focus at the cost of the BV focus? Because monetary revenue is often not the focus of information systems management, governance of risk is often considered a role in which accountability of costs matters, not revenues or profits. On the other hand, governance of opportunities is often seen as a revenue, profit or investment center. These perspectives often cause different reactions because cost control is predominantly centered on a budget rather than a strategic plan.17

The dichotomy—resources and processes vs. BV—may cause one to perceive the governance of risk as a domain logically separate from the governance of opportunities. Tensions between the two focuses may heighten the challenge of keeping the two in alignment. For example, outsourcing some of the transaction processing systems to an offshore vendor could be an opportunity for huge cost savings annually. As management considers this an attractive option to lower costs and improve profits, it should also tackle related issues present in the governance of risk. For example, who owns client data, how secure are these data and what happens if in the future the client company wants to exit the outsourcing arrangement?18 Clearly, the governance of risk is not separate from the governance of opportunities, although it may appear so in some instances in which the issue is almost exclusively either of risk management related to resources and processes (with the creators of information) or of opportunity leverage (with the actors of information).

Regardless of the impact on either type of governance, a careful evaluation of both should be undertaken jointly by the managers responsible for the areas of risk and for opportunities. The guidance suggested in the first myth also applies here. Moreover, the Responsible, Accountable, Consulted and/or Informed (RACI) chart recommended and illustrated in the COBIT framework is an effective integrating mechanism to overcome this misunderstanding.19 COBIT 5 articulates how enterprise goals that signify business value cascade into IT-related goals targeted to mitigate resources and processes risk areas.20
MYTH 5: GOVERNANCE IS AN ALL-OR-NOTHING PROPOSITION

Looking at elaborate frameworks such as COBIT, one may be impressed and puzzled at the same time. COBIT is a powerful framework that cannot be brought to its full potential within a short period of time. It will take a prolonged period of time to set the framework right. Such a challenge may tempt some people to quit altogether because the task of implementing the framework looks imposing. On the other hand, any controls that may be in place in the absence of the rigor of a control framework may be random, deficient in design or operation, and collectively spotty. To identify and fill the voids, the use of a control framework is essential. To abandon the adoption of a control framework would be counterproductive in the long run. Even if the benefit of a control framework is in doubt, publicly traded companies in the US are subject to legal requirements to implement an appropriate framework for internal controls related to their financial systems.

Whereas a control framework is a crucial requirement for disciplined risk management, it may not be necessary to work through every objective of each domain concurrently. As long as a broad map is drawn and the overall view is clear, it would be appropriate to address first those objectives in which a serious lack of control effectiveness exists. Once risk exposures are rated and prioritized, it becomes feasible to prioritize action items. This is much like deploying a divide-and-conquer approach that allows for a step-by-step implementation of controls and that, over time, leads to the implementation of almost an entire control framework. Local initiatives to identify and address control objectives also reinforce a culture in which risk management is everybody's business, not just the CRO's. While a top-down approach to plan for an implementation of a control framework is almost a requirement, the implementation sequence of specific control initiatives may not follow this path. As long as pieces of the puzzle are determined, it could be appropriate, and effective, to fit the identified and prioritized pieces within the puzzle.

To address this negative bias toward information governance frameworks, a program of pilot projects can be used. Executing a pilot project to achieve compliance within a small team, system or area can provide reassurance over the approach, serve as an example for other teams and help dodge associated pitfalls before a framework is implemented organizationwide.21

MYTH 6: GOOD GOVERNANCE WARRANTS NEW TECHNOLOGY

The pace at which technology advances is so impressive that access to new technology is an imperative for organizations. New technology also creates significant comparative advantages in terms of green initiatives, energy savings, productivity improvements and better security. Moreover, technology vendors may, after some time, not support prior versions, and incompatibility between recently acquired technology and existing infrastructure may begin to frustrate both systems and management professionals. For these and similar reasons, adopting new technology may be an attractive option. In summary, as often prescribed, technology is there for business reasons, not for its own sake. The justification to adopt a new technology should come from its BV to the firm. Making the case for the adoption of a new technology purely from the vantage point of the resources and processes focus is likely to be less successful than from that of the BV focus.

For effective governance, the adoption of a new technology is likely, but it is not imperative. Generally, if the mitigation of a particular exposure can be achieved cost-effectively using a new technology that fits the current technology in use, the new technology's adoption can be supported. Clearly, effective governance is not a product of new technology, although it may facilitate or improve governance. If a technology that is vastly different from what exists within the firm is adopted, the governance of risk is likely to pose a bigger challenge.

MYTH 7: GOOD GOVERNANCE REQUIRES SEPARATE FUNDING

Good governance cannot happen without allocating resources; however, the assumption that each governance measure must be supported by separate funding is misleading. In fact, management, using the BV focus, often thinks about what is needed to leverage an identified opportunity; the mitigation of risk emerging from such an action is considered a subset of the same action, not a separate action. Therefore, the expenditure budget for the governance of risk may not change materially every time a new opportunity is exploited by the organization.

A side effect of this management behavior could be that new risk stemming from management decisions is not noticed and, therefore, is not addressed. This may happen
regardless of whether such risk will require additional funding to manage it. One way to force the discovery of risk-related issues and how they will be addressed is to include within the BV justification process a specific question that pertains to the potential impact of the decision on risk related to resources and processes.

CONCLUSION

A clear comprehension of the two focuses of governance—resources and processes that generate information and BV—is a key prerequisite for addressing information governance at any level within a firm. Without understanding the distinction between the two, debates will ensue and different paths will be taken because of unstated assumptions about whether one is looking at risk related to resources and processes or risk related to opportunities (BV). ISACA's recently released COBIT 5 integrates the two focuses into a single view, thus facilitating and simplifying the governance of enterprise IT (GEIT) in a unified manner.

Several myths, or misconceptions, persist because of oversight of this dichotomy and other similar concepts working behind the governance scene. This article outlined seven such myths and, where possible, suggested ways to counter such perceptions. The ERM plans of a firm can become ineffective because of misperceptions or biases, and these should be challenged and removed through systematic communication and orientation so that any drag on the organization's governance initiative is minimized, if not eliminated.

ENDNOTES

1 ISACA, COBIT® 5, USA, 2012, www.isaca.org/cobit
3 Hilb, Martin; New Corporate Governance: Successful Board Management Tools, Springer, Germany, 2005
4 Khatri, Vijay; Carol V. Brown; “Designing Data Governance,” Communications of the ACM, vol. 55, issue 1, January 2010
5 Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management—Integrated Framework, USA, 2004
8 Raval, Vasant; Ashok Fichadia; Risks, Controls and Security: Concepts and Applications, Wiley, USA, 2007
9 Protivity Inc., “Positioning the CRO for Success,” Board Perspectives: Risk Oversight, USA, 2010
10 The scope of governance and management of enterprise IT (GEIT) practices addressed in Val IT and Risk IT are now an integral part of COBIT 5 (www.isaca.org/cobit), such that COBIT 5 can act as the framework by which enterprises can identify the GEIT needs of all stakeholders and balance short- and long-term enterprise goals effectively.
20 For some examples, see ch. 2, p. 21 of COBIT 5, ISACA, 2012.
21 Op cit, Annaswamy