The global economic crisis we have all experienced since the fall of 2008 resulted from a complex set of factors. One of the most apparent causes was flawed management of internal control systems. For example, in Europe, and particularly in France, internal control failures severely impacted Airbus Industrie (a subsidiary of the EADS group) in 2006 and Société Générale in 2008. Both cases marked the need for organizations to manage their internal control and risk management systems more effectively. In the case of Airbus Industrie, the fact that a two-year production delay on the new Airbus A380 went undetected was a clear sign of internal control dysfunction. In the case of Société Générale, the fact that for nearly a year the trader Jérome Kerviel was able to invest tens of billions of Euros unknownst to either external or internal auditors was also a sign of internal control failure. At the same time that these malfunctions occurred, however, operating reports for both companies concluded that internal control and risk management systems were solid and current laws on internal control security were being respected.
In the aftermath of such developments and, on a larger scale, the Enron, WorldCom, and Parmalat scandals, measures have been taken to reestablish investor confidence. Among them, a new series of norms, such as the Sarbanes-Oxley Act (SOX) and its international equivalents (for instance, the Law of Financial Security (LFS) in France), have compelled companies to “institutionalize” methods for managing risks and achieving entity objectives. According to Paul DiMaggio and Walter Powell, “institutionalization” is the process by which social processes take on the status of rules governing corporate thought and action. These new regulations have had tremendous impact on management practices of late. Combined with the climate of economic crisis, such changes have fuelled intense interest in internal control and risk management systems.

This article addresses some of the main questions pertaining to these issues. Could implementation of SOX (or international equivalents such as LFS) and the standardization of internal controls result in the institutionalization of the internal control function within companies? How can companies perform and institutionalize an internal control function most effectively? Is there such a thing as a secure internal control system? To answer these questions, this article builds on the model proposed by Scott Wilkins and Parveen Gupta. They suggested that a project management approach could be an efficient way for companies to organize internal control systems, manage risks, and sustain compliance with SOX Section 404. My purpose is to extend their model by advocating the idea that companies should manage their internal control systems as an ongoing practice, not just as a one-time project designed to cope with SOX 404 or its international equivalents. To this end, I identify organizational and managerial conditions for standardizing the internal control function as a long-term corporate feature.

To address these questions and assess the value of establishing regular processes of internal control, this article draws on the results of action research undertaken by Anthony Buono and Henri Savall. Starting in 2003, they surveyed how 15 European public and private-sector companies with staffs numbering between 100 and 30,000 employees were working to enhance their risk management and internal control systems. To clarify matters, this article will focus on data derived from a single company whose results correlated with the averages among those surveyed. This company is a French surveillance and security concern with a staff of 800, which in turn belongs to a larger U.S. group with a total staff of 30,000. As such, it is representative of the many smaller public companies and foreign entities that are also required to comply with the requirements of SOX Section 404 and its international equivalents.

**Background**

On one hand, internal control is said to help ensure fair and accurate financial reporting, manage risks, and give reasonable assurance regarding the achievement of entity objectives. On the other hand, the explicit goal of SOX is to improve the transparency, timeliness, and quality of financial reporting. The internal control requirements of SOX Section 404 require management to take ownership of internal controls over financial reporting by assessing and publicly reporting on their effectiveness. But because improved controls over financial reporting also have beneficial management effects, SOX has profound implications for internal control systems. Thus it is important for anyone interested in management control systems to understand the main elements of SOX. Zabihollah Rezaee and Michael Holt have explained the many legal sections of SOX, but there are specific components of the Act that are of interest to most companies. Section 108 defines what “accepted accounting principles and practices” are and which are obligatory in a company’s accounting system. Sections 201 and 202 define which services external auditors can perform. Sections 204, 205, and 301 require the establishment of an Audit Committee. Most important, Section 302 requires that CEOs and CFOs certify that their internal control system works and that their reports are correct. In conjunction with 302, Section 404 makes the establishment of an effective internal control system mandatory. Section 406 requires all senior financial executives to sign a code of ethics. Finally, Section 906 calls for periodic reports, stipulates their content, and requires that they contain all pertinent information.

To comply with these standards, most companies have adopted the framework of the Committee of
Sponsoring Organizations of the Treadway Commission (COSO) to create their internal control system. In broad terms, according to the *Enterprise Risk Management—Integrated Framework*, a company first needs to establish a “control environment” that sets the tone for the entire organization and increases control awareness within its staff. It should then perform a company-wide “risk assessment.” In addition, it should formulate “control activities,” i.e., policies and procedures that help ensure that management directives are carried out. Moreover, it should institute a “monitoring system” to verify that the foregoing activities are carried out and adhered to.11

To accomplish these objectives, each company needs to structure systems that coordinate, record, control, and archive the myriad activities that company employees perform in order to accomplish corporate objectives. Finally, it is necessary to appoint an internal auditor or audit team to monitor the internal control system and ensure that it is complete.12

Rezaee and Holt stress that SOX norms are only binding on reporting or public corporations.13 But the effects of SOX have far-reaching impact on private companies and small businesses as well. The main reason is that there is now intense public awareness of the need for good corporate governance on the part of every business. Banks, accountants, insurers, government contract issuers, and other shareholders want to know that every company they are dealing with is managing itself legally and effectively. Regardless of a company’s size, planning, executing, and sustaining an internal control assessment under Section 404 is a challenging and costly project.14 Although much has been written about the difficulty of complying with the new internal control certification requirements, few articles have focused on providing guidance about how to sustain compliance and manage risks in a cost-effective manner. A notable exception is the contribution by Wilkins and Gupta. By using a project management approach and implementing several additional practices, they explain that companies can devise a compliance project that is not only economical but that also helps achieve better business results. To this end, they propose a SOX Project Governance Model including a compliance steering committee led or sponsored by the CEO and the CFO. For Wilkins and Gupta, it is critical that a company’s senior leadership insist on a top-down, risk-based assessment approach. In their view, this is the only way that a company can maintain cost-effective compliance for the long term.15

Above all, the recent failures in internal control experienced by concerns such as Airbus Industrie and Société Générale show that companies can no longer be satisfied with a periodical “project management” approach toward handling their internal controls over the long run. Indeed, a project management approach is necessarily periodical because it lasts only for the life of the project. Such a method is undoubtedly a useful way to introduce an internal control system in an organization. After implementation, however, an internal control system then requires permanent management in order to constantly maintain and improve it. This is why, in my opinion, the Wilkins and Gupta model must be utilized and extended.

**Theoretical Model**

Henri Savall and his collaborators have shown that the successful management of a function is based on the quality of synchronization, the proper reform and reorientation of the function, and the quality of the information system allocated to it.16 As Rezaee points out, establishing these parameters requires a shift from the traditional method of managing internal control—usually occasional and dependent in nature—to one that treats it as an ongoing function in its own right.17 Research by the Savall group has provided a theoretical model for institutionalizing an internal control function that is continually active (see Figure 1).18

This model involves the following key components.

First, the internal control function is steered by a committee, wherever possible by the internal auditing department, and with the support of the top-management team. This committee oversees all sectors of the company related to internal controls, risk management, and compliance with SOX 404—in particular, top and middle management, management controllers, and quality control and internal audit departments. Each of these elements is responsible for managing its internal control objectives and reporting to the steering committee about ongoing performance. The internal control steering committee is in charge of organizing
quarterly meetings to synchronize all the elements involved with internal controls. These meetings should be aimed at assessing the achievement of objectives, dealing with weaknesses, and sharing best internal control practices across departments. Every six months the steering committee will audit and revise procedures, update objectives, and evaluate the efficiency of each internal control function. This should be achieved by comparing the investments requested by each corporate element, such as time devoted to internal controls, with the outcomes, such as cost cutting resulting from the reduction of dysfunctions and risks.

**Research Methods**

To evaluate how companies manage the stages of this model, Buono and Savall applied a form of action research known as “intervention-research,” also called the Socio-Economic Approach of Management (SEAM). This transformative and field-based approach is well suited to the objectives of observing and describing a company’s internal control system before implementation of SOX and then assessing the managerial actions necessary to implement this law and improve the quality of internal control.

The SEAM intervention method aims to improve a company’s socioeconomic performance. Indeed, the fundamental hypothesis upon which it is based recognizes compatibility between social and economic performance. For instance, Jeffrey Pfeffer and Robert Sutton have shown that social performance and management quality strongly contribute to an organization’s sustainable performance. Basically, the tools and methods of SEAM intervention are organized around three axes: the Tool Axis, the Change Axis, and the Policy Axis (see Figure 2).

The Tool Axis of the SEAM approach is composed of six tools. A periodically negotiable activity contract formalizes the qualitative, quantitative, and financial objectives for the organization. These objectives are broken down and applied by every company employee and then included in contracts during biannual discussions between employees and their immediate superiors. An internal-external strategic action plan is a strategic tool that takes into account both external targets (mar-

---

**Figure 1: Model for the Performance and Institutionalization of the Internal Control Function**

[Diagram of the model with labeled nodes: Internal auditing, Synchronization, Steering, Information, Quality systems, Cleaning up, Administration control, and Management systems.]

---
ket share, customer satisfaction, and maintaining quality suppliers) as well as internal clients (technology, fixed and intangible investments, and training of each employee from the CEO to workers). This plan is reevaluated every year to define the focus of the organization for the coming three to five years. A priority action plan (PAP) is an inventory of priority actions, updated biannually, to be carried out by a group of teams (services, board of directors, management, etc.) in order to attain the organization’s strategic objectives. A piloting logbook combines all pertinent indicators—qualitative, quantitative, and financial—that members of the management team use to direct staff and the activities in their zones of responsibility. A coherent set of time management instruments will facilitate more efficient organization of individual and collective activities by fostering the development of individual and collective scheduling as well as collaborative delegation among all company employees. A competency grid maps out competencies currently available in a team. Each of these tools should be introduced through a collaborative training program mobilizing top- and middle-management teams. The Change Axis of the SEAM method involves managers and lower-level personnel. This axis consists of an iterative process divided into four phases: Diagnosis, Project Development, Implementation, and Evaluation.

An initial phase of socioeconomic diagnosis will reveal weaknesses in a company’s internal control system and the hidden costs they generate. The costs resulting from control dysfunctions are called “hidden costs” because they are not always identified, quantified, or controlled by standard information systems such as budget, general, or cost accounting. Hidden costs destroy value, thereby affecting the overall economic performance of the enterprise. The main diagnostic tool for revealing them is a procedure of in-depth, semi-structured interviews conducted by interveners and focusing on dysfunctions, weaknesses, and failures. Interviews are carried out with every member of the managerial team and with 30% to 60% of all shop-floor personnel. Once all interviews have been completed, the results are presented to the entire group of interviewees gathered in collaborative clusters. According to
the technique known as the “mirror effect,” these presentations will allow participants to recognize insufficiencies and validate the results of the diagnosis.

Based on information provided by the diagnostic process, the next stage entails developing a socioeconomic project that will reduce dysfunctions, improve internal control, and convert hidden costs into value-added. The project is formalized in participatory fashion, with the support of a focus group whose mission is to propose cooperative solutions. Following the development of a socioeconomic project, solutions are implemented using the SEAM management tools. For instance, priority action plans distributed to all the departments concerned will target necessary actions. Each PAP will identify objectives and measures to be stipulated in periodically negotiable “activity contracts” with the personnel responsible for them.

After launching the intervention, a process of comparative evaluation should be carried out. Another phase of interviews with the team of directors, a sample of managers, and a group of shop-floor personnel will permit analysis of the qualitative, quantitative, and financial results obtained.

The third component of the SEAM method is the Policy Axis, which is based on a piloting group composed of the CEO and members of the board of directors. This group defines the orientation of change, including the underlying strategy, “rules of the game,” social policy, choice of participants (in the project group, for instance), and so forth. The Policy Axis stimulates strategic decision making, so top managers must be involved in this process.

Example of a Research Process

The research undertaken by the Savall group utilized these elements of SEAM methodology to assess efforts by 15 European companies to improve their risk management and internal control systems. Let’s now consider the application of these principles in the case of one representative company. The company under consideration sells, installs, and maintains surveillance and security systems for other French companies. Its core business is the sale of surveillance equipment on a subscription basis, with contracts running for a period of four years and paid on a monthly basis. The organization is a French subsidiary of a large American company in the electricity sector. It was founded in the 1990s and has enjoyed steady growth ever since. This growth was supported by strong sales and a strategy aimed at winning as many customers as possible through aggressive sales techniques and a well-designed financing concept. The company had revenues of $100 million in 2004. Since 2003, the company has implemented tight internal control procedures in order to comply with SOX 404, meet American stockholder demands, and adhere to LSF norms in France. (Briefly, there are no significant differences between SOX and LSF standards. At first glance, the scope of LSF may appear to be wider than that of SOX because LSF is aimed at public and private companies while SOX focuses on the former. But, as Holt stresses, even if SOX is only binding on reporting, or public, corporations, its effects extend to private companies and small businesses.)

In order to reach its internal control objectives, this company set up a permanent control function via an eight-step process of SEAM intervention. In the first half of 2003, individual interviews with every member of the managerial team and with 30% of all shop-floor personnel identified dysfunctions of internal control hindering the achievement of objectives. This diagnosis enabled the company to identify weaknesses and failures in its internal control, which was not yet organized as a standing function. Subsequently, two interviews of one hour each were conducted with individual managers to assess the qualitative (i.e., particular regulations transgressed), quantitative (i.e., frequency of occurrence per year), and economic (i.e., resultant loss of added value per year) impact of these weaknesses. The economic impact of these problems was assessed by using the hidden cost method (i.e., evaluating the costs of transgressing regulations). The assessments were grouped according to two types of activity: consumption of products (goods or services) and personnel activity. Goods or service consumption quantities were evaluated according to prices charged to the company. Personnel time was calculated according to Hourly Contribution to Value Added on Variable Costs (HCVAVC). HCVAVC is equal to the ratio of the contribution margin and the planned number of work hours—the contribution margin being equal to turnover realized less variable charges.
(i.e., those charges that vary depending on the level of activity). HCVAVC is an indicator for the creation of economic value in any organization and is just as useful for analysis and management control decisions as it is for strategic steering.

This classification was then developed in economic terms using six components: overconsumption, overtime, nonproduction, excess salaries, noncreation of potential, and risks. Product consumption quantities were evaluated financially based on prices effectively charged to the company. Overconsumption is defined as consumption that could have been avoided. Overtime corresponds to time spent in the enterprise that does not add value (e.g., redoing work due to a mistake), while nonproduction is an absence of activity or work stoppage caused by a dysfunction (e.g., a computer breakdown). Both overtime and nonproduction costs are measured using HCVAVC. Excess salaries are determined in terms of wage differences—for instance, when an activity is done by a person holding a better-paid function than that they are required to perform or when wages are paid to people who are absent. Noncreation of potential can be seen as an opportunity cost for the company, and risks are possible future costs generated by current problems. All of these hidden costs constitute the destruction of value added as a result of dysfunctions in internal controls and therefore affect the overall economic performance of the company.

At the same time it undertook this diagnostic process, the company trained its entire management team in the six tools of socioeconomic management. These tools included: time management, competency grids, piloting logbooks, priority action plans, internal and external strategic action plans, and periodically negotiable activity contracts. Then, in the second half of 2003, the company established project groups in each of its main departments. These groups were charged with proposing solutions for the reduction of dysfunctions and the improvement of internal control within the context of SOX implementation. In the first half of 2004, appropriate solutions were incorporated into PAPs for each of the company departments. Utilization of the six management tools enabled company employees to apply the defined solutions and foster attainment of short-, medium-, and long-term objectives intended to improve internal control. Over the second half of 2004, a subsequent qualitative and economic evaluation of the SOX implementation process and the application of defined solutions was undertaken in the relevant departments. Through every stage of the process, a piloting group composed of the CEO, the financial director, the human resources director, and the production manager met periodically to monitor the intervention and its results.

**Results Achieved During the Diagnostic and Project Group Stages**

The results of this sequence of procedures confirmed the value of the organizational and managerial actions that were implemented to improve internal control and sustain SOX 404 in this company where these components had not been previously organized as regular functions. I first present results achieved during the diagnostic and project group stages; then the results observed at the subsequent stage of evaluation; then I relate the key findings based on these results. The results for each item of internal control are presented in accordance with the COSO model: control environment, risk assessment, control activities, information and monitoring systems, and hidden costs.

The control environment is a pivotal element of corporate culture that determines the level of awareness among personnel about the need for control. The diagnostic process revealed that the control environment of the company suffered from a lack of rigor, professionalism, and ethics on the part of managers and supervisors. To improve the control environment, top management examined the implementation of a number of actions affecting all company managers and, through them, the company's entire staff. First, training-consultation actions were organized to enhance the rigor of management and provide the managers with tools for the management of skills, time, delegation, steering, and the assessment of personnel. Second, management defined the ethical rules of the company more precisely, especially in terms of dealing with personnel and customers. These rules were formulated as specific objectives stipulated in periodically negotiable activity contracts for responsible personnel.

The risk assessment aspect of the diagnosis showed
that the company was confronted by a combination of external and internal risks, such as those associated with the collection of receivables or the interruption of supplies critical to business activity. To better structure its risk assessment system, the company undertook a combination of organizational and human resource actions. First, it recruited a risk manager who was answerable to management and responsible for handling both financial and legal risks—the latter being extremely sensitive in the surveillance sector. Second, at the beginning of each half-year period, the CEO and board of directors presented to all company managers a Management PAP that formalized the objectives of the company over the coming six-month period, the actions to be implemented to achieve these objectives, and the areas of managerial responsibility. Each manager then applied the principles of the PAP in relation to his or her area, service, or team. At the end of the half-year, each manager assessed the implementation of his/her PAP, identifying and explaining any failures to meet targets. By eliciting such bottom-to-top feedback, top management was able to assess implementation of the Management PAP over each biannual period and measure the ongoing achievement of its objectives. Through these procedures, which operated both top-to-bottom and bottom-to-top, the company put into place a decentralized, synchronized, and documented risk assessment and control activity system that functioned at all hierarchical and functional levels and was supplemented by internal audit checks at the demand of top management.

Regarding the company’s information and monitoring systems, the diagnostic stage revealed that the company did not use a unified information system. To rectify this, management undertook long-term actions to restructure the information technology department and place it under the control of the financial director. In addition, it became apparent that the internal control system was not subject to sufficient monitoring but, rather, was part of a passive and diluted system. Monitoring of internal control was therefore reorganized in 2004 through another PAP-driven procedure that made individual managers more responsible and synchronized the process via internal auditing with the support of top management.

Overall, the results of the diagnostic stage revealed very high hidden costs due to failures in internal controls and risk management systems. As a matter of fact, these weaknesses generated significant costs for the organization in the form of overconsumption, overtime, nonproduction, excess salaries, noncreation of potential, and risks. An extrapolation of the average amount of hidden costs per person estimated the total amount of the company’s hidden costs at $38 million for 800 people in 2003.26 Clearly, this constituted the destruction of value added stemming from internal control system inadequacies.

**Results Observed at the Evaluation Stage**

Upon consideration after the initial diagnosis stage and subsequent application of corrections via project groups and PAPs, it is clear that the internal control reforms undertaken by this company were successful. After three semiannual periods (second half-year of 2003, first and second halves of 2004), observations confirmed that the company achieved a satisfactory level of control over its internal control systems, verifying the depth of the managerial and organizational changes undertaken. At the end of 2004, external and internal auditing confirmed that the company was in line with both SOX and LSF requirements. During the second half of 2004, an evaluation of the efficiency of the internal control function was also undertaken according to the hidden cost method.27 Costs incurred by the internal control function were evaluated by adding investment expenses (e.g., the new information system and the costs of training sessions) and operating expenses (e.g., time spent by managers on internal control activities). Benefits reaped by the new internal control function were evaluated by measuring the reduction of hidden costs through internal control improvements. This evaluation revealed that the total cost of the internal control systems was nearly $8 million a year. At the same time, however, the reduction of hidden costs through the improvement of internal control systems came to nearly $16 million a year, linked mainly to the decrease of overtime, nonproduction, overconsumption, and risks. This evaluation confirmed that improving the quality of the internal control system by managing it as a primary function of the enterprise did help sustain SOX 404,
manage risks, and, at the same time, reduce hidden costs and losses of added value.

**Key Findings**

These results confirm that a well-organized internal control system can contribute significantly to an organization’s overall performance. There are several key findings from this case study: It is clear that internal control should be organized as a standing function of the organization. Moreover, assessments made during the implementation of SOX indicate that the normalization of internal control is best facilitated by the institutionalization of an internal control function, i.e., by putting into place permanent mechanisms and tools for reform, direction, and synchronization of internal control.

The company achieved these goals by following a model in which the managers of administration control, quality control, and internal auditing acted in a synchronized manner to identify negative and positive points of internal control. Negative elements became the targets of corrective actions incorporated into PAPs for managers at every level. The organization thereby focused on specific risks through a combined top-down and bottom-up approach. With the explicit support of the company’s board of directors, semiannual assessment of PAP implementation verified increases in the overall quality of internal control. The positive economic impact achieved by enhanced internal control efficiency ensured the ongoing commitment of the board of directors. As a result, the process became a regular function of the company, guided and synchronized by internal auditing with the support of top management and the involvement of managers at every level.

Thus, this investigation of a single company as representative of 14 other action research cases confirms the key elements and principles of the model proposed for the performance and institutionalization of an internal control function, namely:

- The internal control function was steered by a committee supported by the top-management team and internal auditing.
- All elements of the company concerned with internal controls, risk management, and compliance with SOX 404 were involved.
- Each area responsible for internal control objectives had to report on the performance through suitable tools, especially PAPs and piloting logbooks.
- Internal auditors were in charge of organizing quarterly meetings dedicated to synchronizing all activities related to the internal control system. These meetings were aimed at assessing the achievement of the objectives, dealing with weaknesses, and sharing best practices across departments.
- Every six months, internal auditors refined the objectives of internal control, revised procedures, and evaluated the efficiency of the internal control function. This was achieved by comparing investments required by the system with outcomes such as reduction of hidden costs and risks.

**The Proposed Model**

Based on analysis of a single case study, these findings do not have statistical validity, but they do enable us to set forth some hypotheses as the basis for further discussion. First of all, this model confirms the main steps of the Wilkins and Gupta Project Management Approach for sustaining SOX 404:

- The explicit support and continued commitment of a company’s board of directors, CEO, and CFO are absolutely essential to starting and sustaining a SOX 404 compliance project.
- Determining the scope of the SOX compliance project annually based on regular evaluations is one of the most important measures that a company can apply.
- Having a SOX steering committee is a key to success for midsize to large organizations.

This investigation also indicates that Wilkins and Gupta’s Project Management Approach can be extended in four important ways:

- The internal control system should be organized as a permanent function, decentralized toward managers, and synchronized by regular internal auditing.
- It should be developed via both top-down and bottom-up approaches with the continued commitment of a company’s board of directors.
- It should synchronize organizational strategy with internal control objectives through common management tools such as PAPs.
It should regularly evaluate the efficiency of the internal control function to confirm that it is organized in a cost-efficient manner. This can be done by comparing the cost of the function with the gains it generates, i.e., the reduction of hidden costs and losses of added value engendered by improved internal control systems.

Finally, it is also apparent that this model will help smaller public companies follow COSO guidelines for monitoring internal control systems.29 While COSO recommendations emphasize that the characteristics of smaller companies provide significant challenges for cost-effective internal control—especially resource constraints—smaller companies usually can meet these challenges and succeed in attaining effective internal control systems in a reasonably cost-effective manner. My model for the performance and institutionalization of the internal control function may be a solution for attaining these ends. Moreover, the tools and devices used to institutionalize internal control procedures, such as PAPs, will help auditors certify that the internal control systems are organized efficiently and effectively. This is certainly an area of research worthy of exploration in further studies.

The Model Works

The recent collapses of insufficient internal control systems such as those of EADS and Société Générale in France, the application of SOX 404 and its international equivalents, and the latest COSO guidelines30 all point to the necessity of institutionalizing internal control functions. Moreover, the worldwide economic crisis since 2008 has made it clear that transforming management of internal controls and risks from an occasional process to a permanent corporate function is a major organizational challenge that should be met by all companies.

This article has proposed and tested a model for performing and institutionalizing an internal control function that will sustain SOX 404 and manage risks. The analysis of a representative case study has confirmed that effective and efficient application of this law and its international equivalents can help companies achieve the all-important objective of restoring investor confidence. It demonstrates that internal control should not be treated as an occasional and dependent procedure but should be institutionalized as a continual management feature. Doing so involves establishing permanent mechanisms for diagnosis, implementation, and evaluation. Specifically, the system should coordinate organizational strategy with internal control objectives with full support of a company’s board of directors, synchronization by a steering committee, and direct involvement of all managers. ■

Endnotes


