SECURINFO for SAP

Guideline for Independent Directors, Senior Executives and Officers

Integrating Corporate Governance Practices with Internal Controls in SAP

Contents

Copyright

Trademarks

If you are a director, senior executive or officer of a company, which is listed on any Stock Exchange, or is considering such a listing, then assurance of compliance with sound Corporate Governance practices should be near the top of your agenda.

Legislation, such as that set forth in America's Public Company Accounting Reform and Investor Protection Act (Sarbanes-Oxley Act of 2002 – "SOX") and guidelines, such as England's Turnbull Report ("TURNBULL") have and are being issued by the various Accounting regulatory bodies and by the various stock exchanges across the world so as to regulate Corporate Governance.

Purpose

This White Paper has been prepared for directors, managers and officers of those enterprises that use SAP and who wish to take straightforward steps towards complying with legislation and guidelines, as well as those who are interested in the practicalities of good risk management and internal control and in getting added value for their companies as a result of compliance.

For directors, the task ahead is to implement control over the wider aspects of business risk in such a way as to add value rather than merely go through a compliance exercise. There is also a need to get the buy-in of people at all levels of the organization and to focus on risk management and internal control in such a way as to improve the business.

This paper has been prepared by people knowledgeable in the practicalities of risk management and internal control particularly as it relates to SAP systems and aims to be a source of timely, practical help to those directors who wish to take steps to implement the new guidance in a straightforward way which brings business benefits.

Content

This White Paper does not go into all of the detail of, and neither does it guide you through all of the issues raised when complying with the legislation or guidelines. It is suggested that the you consult your professional advisors when doing so.

Responsibility of the Board

Shareholders, potential investors and other interested parties rely on information disclosed in a company's financial statements, which are approved by the board of directors prior to issue. The various guidelines recognise that board members relyon information from management, auditors (both external and internal), and experts on major issues when approving these disclosures and SOX sets out the issues which require their attention before they can do so.

Financial Statement Certification

SOX stipulates corporate responsibility for the financial statements and requires a statement from the CEO and CFO to accompany the audit report and certify the "appropriateness of the financial statements and disclosures contained in the periodic report, and that those financial statements and disclosures fairly present, in all material respects, the operations and financial condition of the issuer."

Audit Committee Responsibility and Independence

SOX places the responsibility to oversee the independent evaluation process of disclosed information squarely on the shoulders of the Audit Committee – "The audit committee of an issuer shall be directly responsible for the appointment, compensation, and oversight of the work of any registered public accounting firm employed by that issuer". SOX states that Audit Committee members shall be members of the board of directors and shall be independent. "Independent" is defined as not receiving, other than for service on the board, any consulting, advisory, or other compensatory fee from the issuer, and as not being an affiliated person of the issuer, or any subsidiary. The emphasis on independence is to assure a fair and objective evaluation of the condition of internal controls governing the process and the integrity of the information being reported.

Audit Committee to Prevent and Detect Fraud

The American Institute of Certified Public Accountants considers that the primary objective of the Audit Committee is to prevent and detect material fraud and errors and ensure audits provide reasonable assurance that the corporation's financial statements are fairly stated in accordance with Generally Accepted Accounting Principles (GAAP).

In past years public accountants placed emphasis on the word "material" when incidents were missed and not discovered in the course of audits. If the incident did not dramatically affect the financial standing as presented by the firm then it was rationalized. Therefore, auditors would not spend much of their limited time investigating such transactions when rendering an evaluation of the company's financial statements. However materiality is no longer a safe curtain available for auditors. Instead there must be active programs and processes to make sure the corporation is preventing and detecting fraud.

Staff Independence

Many companies have filled key management positions such as Chief Accountants, Controllers, and CEO positions with personnel who were associated with the company's external audit for many years. This has sometimes led to the emergence of a "farm club system" whereby External Audit personnel were repeatedly promoted into key positions within the company. Companies should establish policies to govern the circumstances and procedures for placement of personnel from the audit firm into key positions of the company, especially after their involvement on the audit.

SOX makes recommendations in respect of the establishment of hiring practices in respect of former Public Accountants. Specifically the CEO, Controller, CFO, Chief Accounting Officer or persons in an equivalent position cannot have been employed by the company's audit firm during the 1-year period proceeding the audit. If a person is trying to gain favourable management support for securing a future position, his independence and view of transactions and operations may be impaired. This “cooling off” period between the person’s audit participation and actively assuming a management role will at least allow the company and audit firms to have a better appearance of “independence” from the people rendering an opinion on the financial reports.

Auditor Independence

Many years ago, audit fees were the primary income of Public Accounting firms. Over the years ancillary services that help give the company specialist expertise in areas like taxes, and new technology have grown significantly and the fees charged for them are often far bigger than the audit fees. Most accounting firms offer a plethora of ancillary services such as internal audit outsourcing, accounting services, systems design and implementation, and risk assessment and abatement services. Audit firms are often under pressure to reduce audit fees and, in an effort to stave off competition, they have tended to reduce audit fees and recover the revenue through ancillary work.

When faced with fee resistance from a client, firms have tried to lower costs by replacing senior people on the audit with lower level personnel. The quality of the review and experience has suffered however, sophisticated methods to record the past and submit to quality reviews helped justify this move by accounting firms. But the bottom line is there was a slow decline in the quality of the review and the independence status of the auditor.

Conflicts of interest arose when the accounting firm partner was faced with internal control weaknesses, differing interpretations of accounting policies etc. that resulted from their own ancillary work.

These conflicts were partially addressed when the major firms split their consulting arms and audit functions in the 1999 and 2000 period. However, many services like risk assessment and security implementation and design were left behind with the audit firms and continue to provide significant income over audit fees. This situation gave way to new legislation and regulations.

The SEC will issue regulations in April 2003 to help renew confidence in the financial reporting process. The requirements will serve as a renewed appreciation for internal controls and pro-active application security programs because it will help fulfil management’s fiduciary responsibility to protect the integrity and completeness of the information disclosed and used to operate their business.

SOX stipulates requirements to determine the independence of the Audit firms conducting the evaluation of the statements and SOX specifically prohibits the provision of non-audit services by the Audit firm contemporaneously with the audit. These include bookkeeping or other services related to the accounting records or financial statements of the audit client; (2) financial information systems design and implementation; (3) appraisal or valuation services, fairness opinions, or contribution-in-kind reports; (4) actuarial services; (5) internal audit outsourcing services; (6) management functions or human resources; (7) broker or dealer, investment adviser, or investment banking services; (8) legal services and expert services unrelated to the audit; (9) any other service that the Board determines, by regulation, is impermissible. Any other services ancillary to the regular audit and not listed above must be pre-approved by the Audit Committee and disclosed in periodic financial reports.

Maintenance & Review of Internal Controls

Information used in the preparation of a company’s financial statements is derived from the information and financial systems. The various legislation and guidelines place responsibility squarely on the shoulders of the board of directors for the

maintenance and review of a sound system of internal control over these systems so as to safeguard shareholders' investment and the company's assets, including the prevention and detection of fraud.

The board should set appropriate policies on internal control and seek regular assurance that will enable it to satisfy itself that the system is functioning effectively. The board must further ensure that the system of internal control is effective in managing risks in the manner, which it has approved.

Reviewing the effectiveness of internal control is an essential part of the board's responsibilities. The board will need to form its own view on effectiveness after due and careful enquiry based on the information and assurances provided to it. Management is accountable to the board for monitoring the system of internal control and for providing assurance to the board that it has done so.

Importance of Internal Controls and Risk Management

The legislation and guidelines communicate that a company's system of internal control has a key role in the management of risks that are significant to the fulfilment of its business objectives. A sound system of internal control contributes to safeguarding the shareholders' investment and the company's assets.

Internal control facilitates the effectiveness and efficiency of operations, helps ensure the reliability of internal and external reporting and assists compliance with laws and regulations. Effective financial controls, including the maintenance of proper accounting records, are an important element of internal control. They help ensure that the company is not unnecessarily exposed to avoidable financial risks and that financial information used within the business and for publication is reliable. They also contribute to the safeguarding of assets, including the prevention and detection of fraud.

A company's objectives, its internal organization and the environment in which it operates are continually evolving and, as a result, the risks it faces are continually changing. A sound system of internal control therefore depends on a thorough and regular evaluation of the nature and extent of the risks to which the company is exposed. Internal Controls should be embedded in the business processes by which the company pursues its objectives.

Since profits are, in part, the reward for successful risk taking in business, the purpose of internal control is to help manage and control risk appropriately rather than to eliminate it.

Internal Control Statements

SOX requires each annual report of an issuer to contain an "internal control report", which shall:

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contain an assessment, as of the end of the issuer's fiscal year, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting. This assessment is subject to audit and will be reported on.

SOX also direct the SEC to require each issuer to disclose whether it has adopted a code of ethics for its senior financial officers and the contents of that code.

Penalties

The significance of Enron, Tyco, and other corporations' financial status has presented a high profile and elevated the accountability of due care to the board of directors. It is expected that compliance will affect the return of shareholder confidence to Corporate America. Severe penalties can be levied on organizations convicted for non-compliance and on the directors and officers. Convicted organizations will be subject to stiff penalties, Examples of financial penalties are:

- Forfeiture of management compensation

following financial statement restatements

- Barring persons from serving as officers or directors of public companies
- Freezing of extraordinary payments made to management while investigations are pending

Prison sentences have been increased even doubled, for convicted persons.

The director's attention to compliance matters is encompassed by fiduciary duty of care responsibilities. Chief Justice Veasey of the Delaware Supreme Court in the Caremark case mentioned the following elements for directors in an attempt to answer two questions:

- What kind of compliance program needs to be established to fulfill duty of oversight?
- How far must directors go to fulfill duty of disclosure?

Corporate governance depends on professionalism of directors and when directors take their job seriously they should not have to worry about liability. However, it is highly probable this case will be applied in future cases given the recent scandals and collapses, with speculation on the potential fines in the millions of dollars.

Audit Committee

The Audit Committee is responsible for overseeing the integrity of the financial reporting process, and is expected to serve as point of collaboration between management, audit and the board. This is clearly a paradigm shift from the reactive practices of the past to a more proactive role in the new era of corporate governance. The following sections reveal challenges and implications to serve in the new era of corporate governance.

When Internal control issues were presented previously by internal and external auditors, board members relied on the auditors and didn't worry about management conflicts. Under the new era, they are the collaboration point to resolve weaknesses and differences between audit and management. Consequently, the integrity of internal controls to provide timely discovery and resolution of issues that affect the financial reporting process are paramount to their fiduciary responsibility. There is an opportunity for not only board members, but also management to be more participative in this area. Internal Controls that are not enforced and supported by management are high risk for non-compliance surprises and weaknesses.

Consequently processes that keep vigilant evaluation and improvement should help abate risks to board member fiduciary duty of care responsibilities. Director and Officer Liability premiums are skyrocketing because of the unknowns for future violations and liabilities. However, insurance companies are going to be receptive to companies who take positive steps to encourage pro-active compliance and discovery processes.

Internal Control Management

Since the 1977 Foreign Corrupt Practices Act, management has had to disclose on the adequacy of internal controls. The recent scandals and collapses tell us some were paying attention to the letter instead of the spirit of the law. Management must be encouraged by Audit Committees to incorporate the enforcement of control processes into their daily operations.

Generally, the involvement of management was to respond to audit reports and recommendations and monitor resolution of weaknesses. Pro-active involvement is the exception not the rule. Much of the emphasis on technology applications over the past few years has put a lot of the internal controls in the hands of technology managers. Conditions can be discovered faster with technology or they can go wrong quickly! In addition, there are very few mechanisms available to provide management the status of controls.

Management will want to become more educated when they certify the adequacy and incur liability and potential penalties for weaknesses that may be discovered after the fact. In some environments, the legal approach will be to get people at the lower levels to certify their operations as adequate and continue up to the C-levels. The presence of "paper" may satisfy perceived liability issues, but the real proof will be how well the company enlightens its staff about the importance of controls and ethics and to what extent management helps by reinforcing controls and ethics. This is no longer an audit issue. This is a business issue.

Application Security

One of the biggest deterrents is a good application security policy and implementation to enforce and support the policy. For example to make sure approval and modification of transactions are not performed by the same person. Or to make sure adjusting entries to financial statements are only in the hands of a select few individuals.

Some of the fundamental controls suffer from management apathy. For example, security is a common internal control that has grown in visibility but still suffers from both apathy and lack of participation. Security of the physical assets, personnel, and information assets are usually all handled by a separate entity but provide the basic

protection. Only 20% of corporations have named Chief Security Officers in their organizations to address the architecture and policies governing all these areas. In essence, there are a myriad of services and vendors available to solve issues. Many companies solved these issues in the past by reacting to problems. When viruses disrupted operations, virus detection software was purchased. When equipment was lost, smart card access systems were installed to monitor entry and exit by authorized staff.

A recent survey by the research firm TheInfoPro indicates that most of the organizations spend less than 3% of their total technology budget on security. The function is viewed as a technical, administrative function except for the policy creation activities. Here is a quote from a Chief Security Officer: “Security gets little attention from the employee and less enforcement from management.” It is essential that security become a business issue. Board members can provide the impetus for more active awareness and support..

Technical vs. Business Perspectives

Many of the application security staff are in the technical support teams in the Chief Information Officer’s organization. They were placed there because all the other security for firewalls and networks were also handled there. However, application security controls what people do across the enterprise. The first problem with a centralized approach is the required liaison between business and technical security personnel to translate business requirements into technical terms. However, the people who are actually accountable and who should manage the risks are the business personnel. This is very seldom the case. Instead technical people dwell on the technical hurdles rather than facilitating the business processes. As a result the business personnel are never sure if their requirements are really implemented without some means of independent verification.

In a recent Harvard Business article the following was revealed about eliminating IT’s grip on business controls:

"Business unit managers are increasingly looking outside the company for the information sharing that is crucial to value creation." Among their specific requirements:

- access to competence throughout the entire network of partners
- the ability to provide efficiency and innovation at the same time
- the ability to design a co-creation process that includes suppliers and customers

What business units need, in other words, is not information, but actionable insights. Such knowledge is contextual; it requires answers not just to what but also to where and when. The challenge today is to manage risks while growing trust.

In a recent evaluation of Enterprise Resource Planning Software projects, a common pitfall was lack of accountability over data. Differences in commonly used data—such as customer and component information—may have historically been shielded by the existence of non-integrated applications. When the data becomes available to the enterprise, project managers should develop an approach to resolving and defining ownership of critical data elements. Once established, Security can enforce the ownership assignments and serve the owner as a management control to make sure the capabilities and assignments are properly maintained.

IT managers often get bogged down in the technical workings and try to make their customers happy rather than addressing some of the difficult decisions to ensure the customer in the business really understands the implications of their decisions. The ability to step up to these important issues creates winners and losers. The key is to recognize when this is relevant and to have a process in place for making these decisions. People need to understand how and why a decision has been made and, importantly, that it will be adhered to. Implementations get bogged down when the business tries to get the technologist to do cartwheels and or IT ignores the business and dwells on technical hurdles rather than trying to solve business issues.

Effective Security Management

Information security involves virtually every aspect of an organization. Unfortunately, centralized security staff deals with most of the day-to-day decisions on who is assigned what capabilities because the mechanisms used to effect the change are technical tools. However, the most effective management systems are those that allow the person closest to the business operation to make the decision. By removing the technical complexity and giving the business manager the tools to effect the decision you get accountability and remove the risk of misinterpretations and hand-offs between the businessperson and technical administrator.

No security policy is worth writing unless it is supported by methods to enforce compliance. There are many blueprints for security policies however, automated tools can help keep up with the volume of activities in managing application processes. The implementation of a process to monitor compliance must encourage integration with day-to-day operations so security is lived each day by everyone in the organization.

Security personnel should think and speak like business people - not technologists. Senior Management want to hear common language that makes business sense, which they can relate to. It is important that senior management understands what their information systems are up against and what there is to lose. Risks need to be managed but unless they are understood, they will be ignored. Reporting industry trends, and the status of your own risk management program will help them make informed business decisions.

Show value. Demonstrate how money, time and resources being spent on information security can help the business avoid surprises. Integrity of the information you are protecting builds confidence in the accuracy of information reported to customers, partners, and shareholders. And most of all helps managers rely more on the information they use to make decisions each day. Many federal regulations can be met as a result of good information security practices. You can even show how information security can play a role in, and even make or break, the success of new projects.

Finally, show that security does not have to be a hindrance to the business. Show them case studies and examples of how it can be a business enabler and integrated with the organization's mission. Be a good listener and treat concerns and objections as requests for more information. Be prepared to respond to these issues appropriately and prove that information security is better than the alternative.

Management Priorities

What management does not know about information security can and will hurt them. No claim can be made to customers, shareholders or even the government that due diligence has been performed if best practices are ignored or if the information security function is simply delegated to the IT team and forgotten. Securing information assets is ultimately management's responsibility, and they must support security efforts. Senior management approves the budgets and signs the checks, and information security must be on their radar. By communicating in a non-technical, business-focused way, security provides the foundation for a truly successful program that enforces management policies, laws and regulations.

There must be a concerted effort in the company to get the major issues to management and the board so as to provide assurance that important internal controls like security are working to protect the integrity of the financial information being reported. If left up to IT personnel, application security will be administered to render the fewest complaints. Consequently, ownership and standards enforcement will take a second seat to quick service and giving people what they want instead of only what they need.

Mission Critical

SAP systems are extensive and usually control most of the companies' financial data. They are mission critical to the business.

Management's responsibility

Management bears the responsibility of ensuring the design, implementation and ongoing monitoring of a sound system of internal controls that are integrated into the day-to-day activities of the company. There are literally thousands of different functions available in the SAP System and directors and officers require assurance that the right people have the right permissions to protect the integrity of the information. Not too much, not too little. Most companies experience difficulties with security in their SAP environment because of the complexity. This complexity combined with a lack of tools in SAP result all too often in a security status that contains many serious but hidden risks.

Solution for SAP Application Security

Securinfo: The Only Complete Solution for SAP

Securinfo's solution has been developed to enable directors and officers to comply with their obligations under the legislation and guidelines. Securinfo allows management, security, and business process personnel to apply their knowledge of SAP functionality, control requirements, and the business to help simplify, accelerate and control the security process. Unlike competing products that only solve one aspect of the issue, Securinfo provides one complete solution with a quick ROI for companies moving to role-based security, completing an upgrade, consolidating multiple locations, or redesigning their SAP security.

Securinfo: Promotes Accountability

Securinfo's solution promotes accountability through a standard methodology of "Information Ownership". This "Information Ownership" is a unique, common sense approach that makes security a business issue not a technical issue. The solution facilitates awareness and understanding of security across the enterprise and makes business accountable for the capabilities and assignments to individuals. Securinfo supports this methodology with very powerful yet extremely easy to use software. The software literally empowers non-technical persons in the business areas of the enterprise to be responsible for the design, implementation and ongoing management of security over data that is relevant to the section of the business for which they are responsible. Until now, due to the technical nature of SAP security and the lack of Change Management functionality in SAP they have not been able to take ownership of, and become responsible for security as it relates data emanating from their section of the business. Instead they have had to make use of inefficient and time-consuming request and respond processes to effect changes. Securinfo changes that, capturing decisions at source, removing traditional bottlenecks and negating the likelihood of error. Authorizations can now be managed "in parallel" across the enterprise, by the business process owners.

Securinfo: Enforces Compliance

Securinfo incorporates clever control concepts that enable the enterprise to design and configure central controls to meet enterprise policies. Methods of control can vary by organizational units as well but still be managed to avoid conflicts in a decentralized environment. The solution filters and organizes pertinent information for the business owner, and also prevents inappropriate entries by placing controls over key controlling elements like cost centers or locations. The organization can be assured assignments and changes are approved by the owner of the information and, more importantly, understood by the approver.

Securinfo: Promotes Process Governance

Securinfo also incorporates checks for the organization to avoid segregation of duty conflicts or inappropriate assignments without express approval of the risk by a responsible business process owner. The business process owners know their own areas from a business perspective, understand their own environment, are most likely to make informed decisions and are much better placed to ensure that any exceptions to policy are justified. From an independent perspective, the reasons for any exceptions are documented and available for review by the auditors in their evaluation of the financial report and internal controls.

Once implemented, Securinfo is an integrated part of the day-to-day business operations. Automatic checks are performed by the software, and important manual tasks to maintain accuracy and completeness checks over the reporting process are created and acknowledged so that at any point in time there is a status of the internal controls (both manual and automated) available for inspection by senior management. All changes are managed with a Change Management module. This is not available in SAP and has long been a requirement of business. Change Management forces compliance with the organization's change policies and procedures before automatically processing the (approved) changes in SAP. This module enables senior management, auditors and other interested parties to quickly obtain the assurance they require in respect of the integrity, and confidentiality of the financial reporting process in SAP.

Securinfo is a giant leap forward for senior officers and audit committee members in implementing pro-active steps, which exhibit due diligence efforts to protect the integrity of the financial reporting process. And it does all this while delivering full knowledge transfer, thus enabling the organization to bypass the need for expensive third party consultants and achieve the lowest possible cost of ownership. With Securinfo technology, your organization can quickly solve the SAP application security challenge from a business perspective.

Conclusion

The recommendations contained in the various legislation and guidelines are as follows:

- Do not delay in achieving compliance
- Obtain management buy-in at all levels of the organization
- Prepare a plan
- Identify and communicate clear security, and control objectives
- Prioritize the risks to the achievement of the objectives
- Establish a clear risk management policy and control strategies
- Consult throughout the business
- Improve the business culture where appropriate
- Keep it simple and straightforward
- Monitor continuously
- Avoid audit committee information overload
- Integrate the legislation and guidelines in your management and governance processes
- Aim to obtain business improvement

Contacts

In addition to product demonstrations to customers, Securinfo offers a “Proof of Concept” to customers who are serious about security. We have regional offices in each continent:

- **Securinfo America**
- **Securinfo Europe**
- **Securinfo Asia-Pacific**
- **Securinfo Africa**

For further information:

please visit us on the web at http://www.securinfo.com

or,

send an email to info@securinfo.com

Appendix: Assessing the effectiveness of the company's risk and control processes

(extracted verbatim from "Internal Control. Guideline for Directors on the Combined Code", by The Institute for Chartered Accountants of England and Wales)

Some questions which the board may wish to consider and discuss with management when regularly reviewing reports on internal control and carrying out its annual assessment are set out below. The questions are not intended to be exhaustive and will need to be tailored to the particular circumstances of the company. This Appendix should be read in conjunction with the guidance set out in this document.

1. Risk assessment

- Does the company have clear objectives and have they been communicated so as to provide effective direction to employees on risk assessment and control issues? For example, do objectives and related plans include measurable performance targets and indicators?
- Are the significant internal and external operational, financial, compliance and other risks identified and assessed on an ongoing basis? (Significant risks may, for example, include those related to market, credit, liquidity, technological, legal, health, safety and environmental, reputation, and business probity issues.)
- Is there a clear understanding by management and others within the company of what risks are acceptable to the board?

2. Control environment and control activities

- Does the board have clear strategies for dealing with the significant risks that have been identified? Is there a policy on how to manage these risks?
- Do the company's culture, code of conduct, human resource policies and performance reward systems support the business objectives and risk management and internal control system?
- Does senior management demonstrate, through its actions as well as its policies, the necessary commitment to competence, integrity and fostering a climate of trust within the company?
- Are authority, responsibility and accountability defined clearly such that decisions are made and actions taken by the appropriate people? Are the decisions and actions of different parts of the company appropriately co-ordinated?
- Does the company communicate to its employees what is expected of them and the scope of their freedom to act? This may apply to areas such as customer relations; service levels for both internal and outsourced activities; health, safety and environmental protection; security of tangible and intangible assets; business continuity issues; expenditure matters; accounting; and financial and other reporting.
- Do people in the company (and in its providers of outsourced services) have the knowledge, skills and tools to support the achievement of the company's objectives and to manage effectively risks to their achievement?
- How are processes/controls adjusted to reflect new or changing risks, or operational deficiencies?

3. Information and communication

- Do management and the board receive timely, relevant and reliable reports on progress against business objectives and the related risks that provide them with the information, from inside and outside the company, needed for decision-making and management review purposes? This could

include performance reports and indicators of change, together with qualitative information such as on customer satisfaction, employee attitudes etc.

- Are information needs and related information systems reassessed as objectives and related risks change or as reporting deficiencies are identified?
- Are periodic reporting procedures, including half-yearly and annual reporting, effective in communicating a balanced and understandable account of the company's position and prospects?
- Are there established channels of communication for individuals to report suspected breaches of laws or regulations or other improprieties?

4. Monitoring

- Are there ongoing processes embedded within the company's overall business operations, and addressed by senior management, which monitor the effective application of the policies, processes and activities related to internal control and risk management? (Such processes may include control self-assessment, confirmation by personnel of compliance with policies and codes of conduct, internal audit reviews or other management reviews).
- Do these processes monitor the company's ability to re-evaluate risks and adjust controls effectively in response to changes in its objectives, its business, and its external environment?
- Are there effective follow-up procedures to ensure that appropriate change or action occurs in response to changes in risk and control assessments?
- Is there appropriate communication to the board (or board committees) on the effectiveness of the ongoing monitoring processes on risk and control matters? This should include reporting any significant failings or weaknesses on a timely basis.
- Are there specific arrangements for management monitoring and reporting to the board on risk and control matters of particular importance? These could include, for example, actual or suspected fraud and other illegal or irregular acts, or matters that could adversely affect the company's reputation or financial position?

References

Wall Street Journal, “Lawmakers toughen rules, but toughness can’t be legislated”; by Jonathan Weil and Dennis Berman.

Fullbright & Jawarski, LLP brochure “Corporate Governance Issues” by Charles Henry Hill, October 2002.

TechTarget: Search SAP article, Selling security to upper management by Kevin Beaver, CISSP, 10 July 2002, SearchSecurity.com

“CSOs bring security to their market” By Michael S. Mimoso, News Editor, 16 December 2002, SearchSecurity.com

“Is it time to fire your CIO?” By Harvard Business School, special to SearchCIO.com, 09 October 2002, HBS Working Knowledge

“The state of e-business: Optimism prevails, investment remains flat”, By Matt Hines, News Writer, 23 September 2002, SearchCIO.com

“ERP's payoffs and pitfalls”, By Harvard Business School, special to SearchCIO.com, 23 October 2002, HBS Working Knowledge

“Internal Control. Guideline for Directors on the Combined Code”, by The Institute for Chartered Accountants of England and Wales, September 1999

“Implementing Turnbull: A Boardroom Briefing” by Martyn Jones and Gillian Sutherland of the Centre for Business performance, The Institute for Chartered Accountants of England and Wales, September 1999